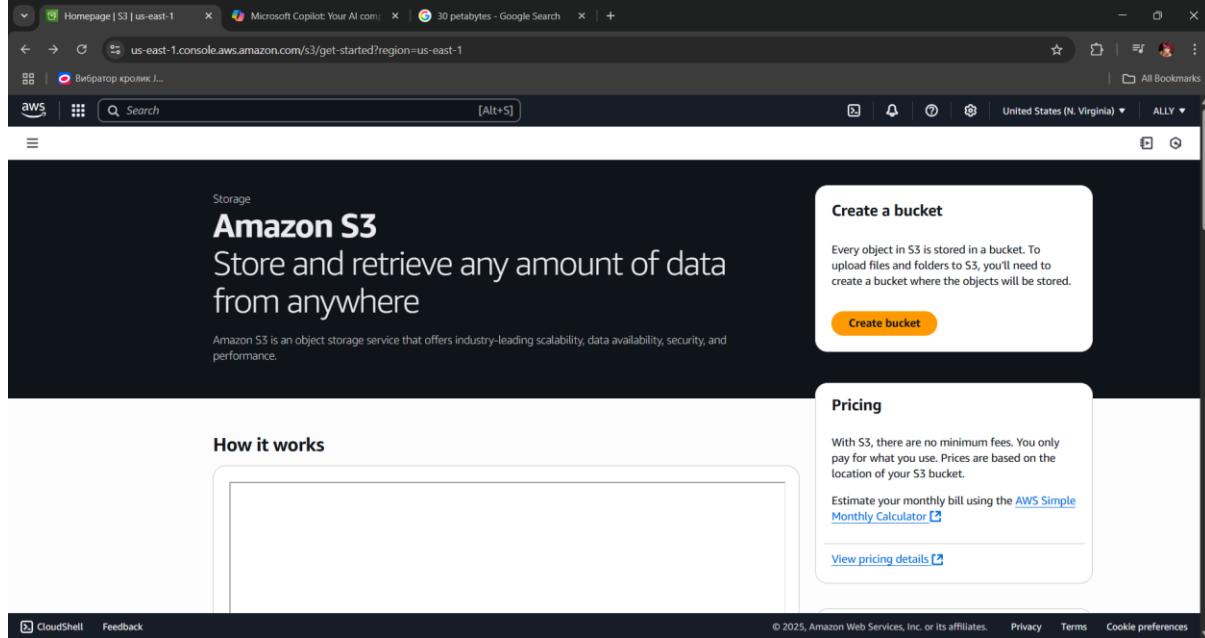


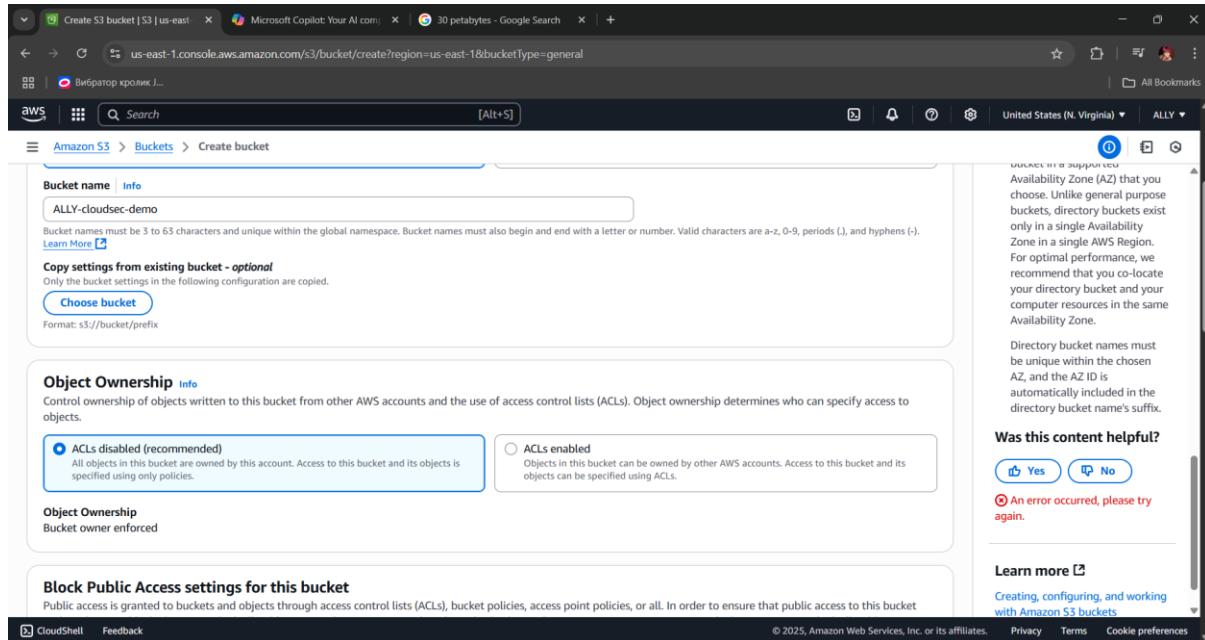
STEPS FOR THE FIRST PROJECT

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



The screenshot shows the Amazon S3 homepage. On the left, there's a large banner with the text "Amazon S3" and "Store and retrieve any amount of data from anywhere". Below the banner, it says "Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance." On the right, there's a callout box titled "Create a bucket" with the subtext "Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored." Below this is a large "Create bucket" button. At the bottom of the page, there's a "Pricing" section with information about no minimum fees and a link to the AWS Simple Monthly Calculator. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

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



The screenshot shows the "Create bucket" wizard. The first step is "Bucket name". The input field contains "ALLY-cloudsec-demo". Below the input field, there's a note: "Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-)." There's a "Learn More" link. A "Choose bucket" button is available for copying settings from an existing bucket. To the right, there's a sidebar with information about bucket naming rules and a "Was this content helpful?" section with "Yes" and "No" buttons. At the bottom, there's a "Learn more" link and a note about creating, configuring, and working with Amazon S3 buckets.

The screenshot shows the 'Create bucket' page in the AWS S3 console. The 'Default encryption' section indicates server-side encryption is applied. Under 'Encryption type', 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' is selected. In the 'Bucket Key' section, 'Enable' is chosen. A note at the bottom says 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.' On the right, there's a sidebar with information about availability zones and a 'Was this content helpful?' poll.

NOTE: Bucket name must not contain uppercase characters

The screenshot shows the 'Buckets' page in the AWS S3 console. A green banner at the top says 'Successfully created bucket "ally-cloudsec-demo"'. Below it, the 'General purpose buckets' section lists one bucket named 'ally-cloudsec-demo'. The 'Account snapshot' and 'External access summary' sections are also visible on the right.

The above is the image after creating the bucket

The screenshot shows the AWS S3 console interface for uploading objects. The top navigation bar includes tabs for 'Upload objects - S3 bucket ally' (active), 'Microsoft Copilot: Your AI com...', and '30 petabytes - Google Search'. The main title is 'Upload objects - S3 bucket ally'.

The page displays the 'Upload' section with the sub-section 'Upload info'. It instructs users to add files or folders to the upload area, which is currently empty. A message states: '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](#)'.

The 'Files and folders' table shows one item: 'Assessing Financial Viability of the l...' (1 total, 16.9 KB). The file type is 'application/vnd.openxmlformats-o...'. Buttons for 'Remove', 'Add files', and 'Add folder' are available.

The 'Destination' section shows the destination as 's3://ally-cloudsec-demo'. Under 'Destination details', it says 'Bucket settings that impact new objects stored in the specified destination.'

The bottom of the screen includes standard AWS navigation links: CloudShell, Feedback, © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

The second screenshot shows the same interface after the upload has succeeded. A green notification bar at the top says 'Upload succeeded. For more information, see the Files and folders table.' Below this, a message indicates that the information will no longer be available if navigating away.

The 'Summary' section shows the upload status: 'Succeeded' (1 file, 16.9 KB (100.00%)) and 'Failed' (0 files, 0 B (0%)).

The 'Files and folders' table now lists the uploaded file 'Assessing Financial Viability of t...' (1 total, 16.9 KB). The file details show it is of type 'application/vnd.openxmlformats-o...' and has a status of 'Succeeded'.

The bottom of the screen includes standard AWS navigation links: CloudShell, Feedback, © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

This is the point I uploaded the file into the bucket

Upload objects - S3 bucket ally

Microsoft Copilot: Your AI com

30 petabytes - Google Search

us-east-1.console.aws.amazon.com/s3/upload/ally-cloudsec-demo?region=us-east-1&bucketType=general

Выбрать кролика...

aws Search [Alt+S]

All Bookmarks

United States (N. Virginia) ALLY

Upload succeeded
For more information, see the [Files and folders](#) table.

Summary

Destination	Succeeded	Failed
s3://ally-cloudsec-demo	1 file, 16.9 KB (100.00%)	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: 41beb6da5616dcba9153ce9db96867cd4578d68576c87e6e4751521a0e76315b	Read	Read, Write

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Upload objects - S3 bucket ally

Microsoft Copilot: Your AI com

30 petabytes - Google Search

us-east-1.console.aws.amazon.com/s3/upload/ally-cloudsec-demo?region=us-east-1&bucketType=general

Выбрать кролика...

aws Search [Alt+S]

All Bookmarks

United States (N. Virginia) ALLY

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

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS S3 console with the URL us-east-1.console.aws.amazon.com/s3/buckets/ally-cloudsec-demo?region=us-east-1&bucketType=general&tab=permissions. The main content area displays an 'Unknown Error' message: 'An unexpected error occurred. Try again later. If the error persists, contact AWS Support for assistance.' A red button labeled 'Diagnose with Amazon Q' is visible. Below this, the 'Permissions overview' section is shown, featuring tabs for Objects, Metadata, Properties, Permissions (which is selected), Metrics, Management, and Access Points. The 'Block public access (bucket settings)' section is expanded, showing a 'Networking error' message: 'Check your internet connection and reload the page.' A red box highlights this error message. At the bottom of the page, there are links for CloudShell, Feedback, and navigation icons.

Encountered some errors when trying to load the permission access panel

The screenshot shows the AWS S3 console with the URL us-east-1.console.aws.amazon.com/s3/bucket/ally-cloudsec-demo/property/bpa/edit?region=us-east-1&bucketType=general. The left sidebar shows 'Amazon S3' with sections for 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) and Block Public Access settings for this account. The main content area is titled 'Edit Block public access (bucket settings)' and shows the 'Block public access (bucket settings)' configuration. It includes a note about public access being granted through ACLs, bucket policies, and access point policies. Under 'Block all public access', there are four checkboxes: 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLS)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. A 'Save changes' button is at the bottom right. The page footer includes links for CloudShell, Feedback, and navigation icons.

Making the bucket accessible to the public

Edit Block public access (bucket settings)

This will result in public access being blocked for this bucket and all objects in the bucket.

To confirm the settings, enter **confirm** in the field.

confirm

Cancel Confirm

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

Successfully edited Block Public Access settings for this bucket.

ally-cloudsec-demo Info

Permissions

Block public access (bucket settings)

Block all public access

On

Individual Block Public Access settings for this bucket

Edit

Successfully made it public

Successfully edited Block Public Access settings for this bucket.

ally-cloudsec-demo Info

Objects | Metadata | Properties | **Permissions** | Metrics | Management | Access Points

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#).

[View analyzer for us-east-1](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Off

[Individual Block Public Access settings for this bucket](#)

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Below is creating user name called junior analyst

Step 1 **Specify user details**

User details

User name

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 providing console access to a person?

Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

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](#)

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create user | IAM | Global Microsoft Copilot: Your AI com... 30 petabytes - Google Search stage four cancer - Google Search javascript - Google Search

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

Выбрать кролика...

Search [Alt+S]

IAM > Users > Create user

User details

User name: junior-analyst

Step 3: Set permissions

Step 4: Review and create

Step 5: Retrieve password

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.](#)

Specify a user in Identity Center

User type: Specify a user

This will take you to the AWS Identity Center console.

I want to create a new user
We recommend creating a new user with specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

[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-east-1 Microsoft Copilot: Your AI com... 30 petabytes - Google Search stage four cancer - Google Search javascript - Google Search

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create

Выбрать кролика...

Search [Alt+S]

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

Выбратор кролик...

Search [Alt+S]

AmazonS3FullAccess 0/0

All Bookmarks

IAM > Users > junior-analyst

Identity and Access Management (IAM)

2 policies added to junior-analyst

Summary

ARN arn:awsiam:...:junior-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.

Filter by Type All types

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

The screenshot shows the AWS IAM Management Console. In the top right corner, there is a green success message box that says "User created successfully" and "You can view and download the user's password and email instructions for signing in to the AWS Management Console." Below this message, the "Users" section is displayed, showing one user named "junior-analyst". The user has a path of "/", an activity count of 0, and no MFA enabled. There are buttons for "View user", "Delete", and "Create user". On the left sidebar, under "Access management", the "Users" option is selected. Other sections like "Roles", "Policies", and "Identity providers" are also listed. At the bottom of the page, there are links for "CloudShell", "Feedback", and copyright information.

Policy of junior analyst

The screenshot shows the AWS S3 Bucket Policy editor. The top navigation bar includes tabs for "Edit bucket policy - S3 bucket", "IAM Identity Center | us-east-1", "Microsoft Copilot Your AI", "30 petabytes - Google Search", "stage four cancer - Google", "javascript - Google Search", and "ghanaweb - Google Search". The main content area shows the policy for the bucket "ally-cloudsec-demo". The policy document is as follows:

```
1 Version: "2012-10-17",
2 Statement: [
3     {
4         Sid: "AllowUserAccess",
5         Effect: "Allow",
6         Principal: {
7             AWS: "arn:aws:iam::730420834930:user/junior-analyst"
8         },
9         Action: "s3:*",
10        Resource: [
11            "arn:aws:s3:::asigbey-cloudsec-demo",
12            "arn:aws:s3:::asigbey-cloudsec-demo/*"
13        ]
14    }
15]
16
17 ]
```

To the right of the policy document, there is a "Select a statement" dropdown and a button to "+ Add new statement". The sidebar on the left lists various S3 features: General purpose buckets, Directory buckets, Table buckets, Vector buckets, 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, and Storage Lens. At the bottom of the page, there are links for "CloudShell", "Feedback", and copyright information.

ally-cloudsec-demo - S3 buckets | 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

Выбрать кролика...

aws Search [Alt+S]

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

CloudShell Feedback

Successfully edited bucket policy.

Bucket policy

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](#)

```
{ "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/*" ] } ] }
```

Copy

© 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

Выбрать кролика...

aws Search [Alt+S]

Amazon S3 > Buckets > ally-cloudsec-demo > Edit server access logging

Enable

Choose destination

S3 Buckets

Buckets (1/1)

Find buckets by name

Name	AWS Region	Creation date
ally-cloudsec-demo	US East (N. Virginia) us-east-1	July 22, 2025, 11:49:31 (UTC+03:00)

[DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
To speed up analytics and query applications, use this format.

Log object key example

Cancel Choose destination

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS S3 console with the path 'Amazon S3 > Buckets > ally-cloudsec-demo'. A green success message box at the top right says 'Successfully edited server access logging.' with a 'Create configuration' button. Below it, the 'Server access logging' section is visible, showing 'Enabled' status and a 'Destination bucket' set to 's3://ally-cloudsec-demo'. A log object key format placeholder '[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]' is shown. The 'AWS CloudTrail data events (0)' section has a 'Configure in CloudTrail' button. The left sidebar includes sections for General purpose buckets, Storage Lens, and IAM Access Analyzer for S3.

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:

Login using the root account (not recommended in production).

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

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

Create a CloudTrail trail that logs activity to an S3 bucket.

Set up an SNS topic and subscribe 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.

What to document:

- Screenshots of all the steps you took
- Screenshot of the CloudTrail log entry for root account activity
- Your SNS topic and subscription configuration
- Screenshot of the alert received via email or SMS
- A short write-up:

"What I did and what I learned

The screenshot shows the AWS IAM Security Credentials page. On the left, there's a sidebar with options like Identity and Access Management (IAM), Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), and Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings). The main content area has tabs for Multi-factor authentication (MFA) and Access keys (0). Under MFA, it shows a table with one item: Type: Virtual, Identifier: arn:aws:iam::[REDACTED]:mfa/ALLY, Certifications: Not Applicable, Created on: Sun Jul 27 2025. There are buttons for Remove, Resync, and Assign MFA device. Under Access keys, it says "No access keys". It also advises against using long-term credentials and provides a "Create access key" button. At the bottom, there are links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

The above is the process of disabling/removing the MFA

The screenshot shows the AWS IAM Security credentials page. In the center, a modal dialog titled "Remove MFA device?" is displayed, asking if the user wants to remove a virtual MFA device. The dialog includes "Cancel" and "Remove" buttons. Below the modal, the "Multi-factor authentication (MFA) (1)" section shows one MFA device listed. At the bottom of the page, there is a "Create access key" button.

Successfully remove mfa below

The screenshot shows the AWS IAM Security credentials page after the MFA device has been deleted. A green success message at the top states "MFA device deleted." The "Multi-factor authentication (MFA) (0)" section is now empty. The "Access keys (0)" section remains, with a "Create access key" button.

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

Выбрать кролика...

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

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

View bill

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

The screenshot shows the AWS CloudTrail home page. At the top, there's a banner with the text "AWS CloudTrail" and "Continuously log your AWS account activity". Below the banner, a sub-headline says "Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts." On the left, there's a section titled "How it works" with two diagrams: "Capture" (showing a cloud icon with a camera lens) and "Store" (showing a cloud icon with a bucket). Below these diagrams, text explains that CloudTrail records activity in AWS services as events and delivers them to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs. To the right, there's a call-to-action box titled "Create a trail with AWS CloudTrail" with a "Create a trail" button. Other sections visible include "Pricing" and "Getting started".

The screenshot shows the "Quick trail create" wizard. The first step, "Trail details", asks to start logging management events by creating a trail with simplified settings. It notes that logs are sent to an S3 bucket created on behalf of the user. A link to the full "Create trail" workflow is provided. The "Trail name" field is filled with "allytrail". The "Trail log bucket and folder" field contains "aws-cloudtrail-logs-730420834930-881d075c". A note states that logs will be stored in "aws-cloudtrail-logs-730420834930-881d075c/AWSLogs/730420834930". A warning message in a box says: "Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs." At the bottom, there are "Cancel" and "Create trail" buttons.

Trails | CloudTrail | us-east-1 | aws.amazon.com | IAM - Multi-Factor Authen... | Microsoft Copilot: Your AI... | Duolingo English Test | IEELS | IEELS Online

us-east-1.console.aws.amazon.com/cloudtrailv2/home?region=us-east-1#/trails

Выбратор кролика...

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

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-1:123456789012:trail/ally_trail	Disabled	No	aws-cloudtrail-logs-123456789012-trail-ally_trail	-	-	Logging

Copy events to Lake Delete Create trail

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create trail | CloudTrail | us-east-1 | aws.amazon.com | IAM - Multi-Factor Authen... | Microsoft Copilot: Your AI... | Duolingo English Test | IEELS | IEELS Online

Выбратор кролика...

CloudTrail > Trails > Create trail

Review and create

Step 1: Choose trail attributes

General details

Trail name allytrail	Trail log location ally-cloudsec-demo/AWSLogs/123456789012/	Log file validation Enabled
Multi-region trail Yes	Log file SSE-KM Enabled	SNS notification delivery 89ca88d8
Apply trail to my organization Not enabled	AWS KMS key alias ally	

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.

If you choose 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 console.

CloudWatch Logs

No CloudWatch Logs log groups

CloudWatch Logs is not configured for this trail

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Trails | CloudTrail | us-east-1 | aws.amazon.com | IAM - Multi-Factor Authen... | Microsoft Copilot: Your AI... | Duolingo English Test | IEELS | IELTS Online

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

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-1:730420834930:trail/ally_trail	Disabled	No	aws-cloudtrail-log-4930-881d075c	-	-	Logging
allytrail	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:730420834930:trail/allytrail	Disabled	No	ally-cloudsec-4930-881d075c	-	-	Logging

Copy events to Lake [Edit](#) Delete Create 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 console. For more information, see Getting started with Amazon SNS.

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Trail details | CloudTrail | us-east-1 | aws.amazon.com | IAM - Multi-Factor Authen... | Microsoft Copilot: Your AI... | Duolingo English Test | IEELS | IELTS Online

us-east-1.console.aws.amazon.com/cloudtrailv2/home?region=us-east-1#/trails/arn:aws:cloudtrail:us-east-1:730420834930:trail/ally_trail

CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:730420834930:trail/ally_trail

ally_trail

General details

Trail logging Edit	Trail log location aws-cloudtrail-logs-881d075c/AWSLogs/ally_trail	Log file validation Disabled	SNS notification delivery Disabled
Trail name ally_trail	Last log file delivered July 28, 2025, 01:20:07 (UTC+03:00)	Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled	Edit	
Apply trail to my organization Not enabled			

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

CloudWatch Logs

No CloudWatch Logs log groups

CloudWatch Logs is not configured for this trail

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS SNS Topics page. A blue banner at the top left indicates a new feature: "Amazon SNS now supports High Throughput FIFO topics. Learn more". Below it, a green banner says "Topic Ally-Alerts created successfully. You can create subscriptions and send messages to them from this topic." On the left sidebar, under the "Mobile" section, there is a "Push notifications" item. The main content area shows the "Ally-Alerts" topic details, including its Name (Ally-Alerts), ARN (arn:aws:sns:us-east-1:...), Type (Standard), Display name (ALLY @ AWS CLOUD SECURITY), and Topic owner (7...). Below the details, tabs for Subscriptions, Access policy, Data protection policy, Delivery policy (HTTP/S), Delivery status logging, Encryption, and Tags are visible. The Subscriptions tab is selected, showing "Subscriptions (0)".

The screenshot shows the AWS SNS Subscription page. A blue banner at the top left indicates a new feature: "Amazon SNS now supports High Throughput FIFO topics. Learn more". Below it, a green banner says "Subscription to Ally-Alerts created successfully. The ARN of the subscription is arn:aws:sns:us-east-1:730420834930:Ally-Alerts:5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0." The main content area shows the "Subscription: 5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0" details, including its ARN (arn:aws:sns:us-east-1:730420834930:Ally-Alerts:5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0), Status (Pending confirmation), Protocol (EMAIL), and Topic (Ally-Alerts). Below the details, tabs for Subscription filter policy and Redrive policy (dead-letter queue) are visible.

CONFIRMED

Subscription: 5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0

New Feature
Amazon SNS now supports High Throughput FIFO topics. [Learn more](#)

Subscription: 5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0

Details

ARN	arn:aws:sns:us-east-1:44cc9d2d07e0	Ally-Alerts:5b708a3c-e94f-4adb-aa2b-44cc9d2d07e0
Endpoint	[REDACTED]	
Topic	Ally-Alerts	
Subscription	arn:aws:iam::[REDACTED]	

Subscription filter policy [Info](#)

Redrive policy (dead-letter queue)

Subscription filter policy [Info](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Create rule > Review

us-east-1.console.aws.amazon.com/events/home?region=us-east-1#rules/create

Amazon EventBridge > Rules > Create rule

Step 1 Define rule detail

Step 2 Build event pattern

Review and create

Step 1: Define rule detail

Define rule detail

Rule name	Hi-AWS_alert-me-when-sign-in-occurs
Description	
Status	Enabled
Rule type	Standard rule

Event bus
default

Step 2: Build event pattern

Event pattern [Info](#)

```
1 {
2   "source": ["aws.signin"],
3   "detail-type": ["AWS Console Sign In via CloudTrail"],
4   "detail": {
5     "userIdentity": {
```

For example, if you wanted to have 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

The screenshot shows the Amazon EventBridge Rules page. A green success message at the top states "Rule LoginAlertRule was created successfully". Below it, the "Rules" section is displayed with the following details:

- Select event bus**: Event bus is set to "default".
- Rules (1)**:
 - LoginAlertRule**: Enabled, Standard type, ARN: arn:aws:events:us-east-1:7...30:rule/LoginAlertRule. Description: Detects root account sign-ins and sends alerts.

The left sidebar includes sections for Developer resources, Buses (with "Updated" status), Pipes, Scheduler, and Integration. The bottom of the page includes standard AWS links like CloudShell, Feedback, and copyright information.

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