To:
The Station House Officer
Cyber Crime, Mohali
Punjab – 160055

Subject: Cybercrime Complaint – Unauthorized Access, Deletion of Proprietary Code, Data Breach & IP Theft.

Respected Sir/Madam,

I am Advocate Akash Sheoran, enrolled with the Punjab & Haryana Bar Council, and authorized legal representative of Mr. GJ Bovrisse, Founder and CEO of Whuups Inc., a US-based technology company. I am writing to file this complaint against :1)Mr. Gaurav Sethi – Co-Founder and CEO, NSL Infotech Pvt. Ltd., 2) Mr. Chirag Kohli – Director/Co-Founder, NSL Infotech Pvt. Ltd. 3) Mr. Jatinder Arora– Director/Co-Founder, NSL Infotech Pvt. Ltd, Plot No. F-547, Phase 8A, Industrial Area, Mohali and other associates for serious cyber offences, including unauthorized access, criminal breach of trust, data destruction, and theft of source code belonging to Whuups Inc.

The following cyber offences have been committed by the accused persons:

1. Unauthorized Access to Whuups Inc.'s GitHub Account

Despite having been officially removed from access, on 21 July 2025, Mr. Gaurav Sethi illegally accessed Whuups Inc.'s private GitHub repository using previously retained or compromised credentials or hacking. This constitutes an unauthorized intrusion into a protected computer system, without the knowledge or consent of the owner. Thereby invoking offence under section 66 of the IT act.

2. Unauthorised downloading of data of whuups inc.

Mr gaurav sethi and his associates have downloaded data (codes etc) of whuups in an unauthorised way and thereby stealing the intellectual property and causing loss to whuups inc. It is pertinent to mention that this data took 5 years of hard work.

3. Deletion of Proprietary Source Code

Subsequent to the unlawful access, Mr. Sethi deleted key source code modules that were developed over multiple months and paid for by Whuups Inc., thereby sabotaging the business and causing extensive data loss and development downtime.

4. Earlier Attempts at Code and Domain Hijacking

Mr. Sethi had previously been warned after attempting unauthorized domain name transfers, as well as illegally hosting Whuups's proprietary code under his personal/NSL GitHub account. A DMCA complaint was filed by the client and acknowledged by GitHub under Ticket ID 3547241 on 8 July 2025.

5. Admission of Unauthorized Transfers

In prior emails exchanged with the client, Mr. Sethi has admitted in writing that he - Transferred the Whuups code to his own company's computer systems and GitHub, Used Whuups's credentials to engage third-party APIs without authority, Retained backend control despite legal instructions to transfer infrastructure.

6. Tampering & destruction of Source Code

That despite the above, NSL and above named accused persons have committed the following wilful and fraudulent criminal acts that include but not limited to tampering & destruction of Source Code and NSL deliberately deleted the functioning peer-to-peer call code which was the complainant's code and broke it and replaced it with old 2022 legacy files, knowingly rendering the core communication module of the app in-operable. This sabotaged years of development costing a tragic loss to Whuups Inc

7. Hijacking Domain name and unauthorised transfer.

That there have been Multiple Attempts to Hijack Domain Name and NSLmade at least two unauthorized attempts to transfer the domain whuups.com to an unrelated registrar (PDR Ltd.), confirmed by OVH logs.

These acts clearly constitute criminal breach of trust, cyber trespass, destruction of digital evidence, and intellectual property theft. Along with the present complaint, I am attaching proof the same with the present application.

I therefore request to you that an appropriate legal action be taken against them. I shall be highly grateful to you.

Akash Sheoran

(Advocate)

Authorised representative of Mr. GJ Bovrisse,

Founder and CEO of Whuups Inc.,

Mob.: 8076770343

Annexure A: Chronology of Events – Whuups Inc. vs. NSL Infotech Pvt. Ltd.

Date	Event
22 Aug 2024	NDA is executed between Whuups Inc. and NSL Infotech Pvt. Ltd., restricting unauthorized access and confidential usage of intellectual property.
03 Nov 2024	First payment of $500 made by Whuups Inc. to NSL, as part of Invoice NSL-INV-24-0007, initiating work in good faith.
06 Nov 2024 – 04 Jun 2025	Multiple payments made by Whuups Inc. totaling **$30,823.71 USD** to NSL via PayPal for mobile/web development.
13 Nov – 13 Dec 2024	Technical issues begin to arise regarding module delivery and NSL insists on further payment without clearing issues.
27 Dec 2024	NSL (specifically accused Gaurav Sethi) tries to steal and attempts to transfer the domain name whuups.com to PDR Ltd. without authorization. OVH (domain registrar) blocks the unauthorized transfer.
Mar–Apr 2025	NSL allegedly begins altering the GitHub repository. Complainant's developed peer-to-peer call code is broken and removed and replaced with outdated versions.
Apr–May 2025	Whuups discovers that critical app features like OTP login and FLIPS integration have not been completed.
May 2025	Gaurav Sethi attempts to access OVH credentials again and makes a second attempt to transfer the domain to PDR Ltd. (email dated 26 Jun confirms prior attempt).
27 Jun 2025	Whuups demands that NSL disclose the API provider for the FLIPS feature and reminds them they are unauthorized to execute licensing under Whuups Inc. name.
01 Jul 2025	Temporary access to Whuups's Apple and Google developer accounts is granted to NSL.
02 Jul 2025	NSL admits in email that call feature was removed and then partially worked on again, but justifies it under platform evolution and accuses the complainant of halting collaboration.
08 Jul 2025	GitHub acknowledges DMCA complaint from Whuups Inc. and registers complaint Ticket ID: 3547241.
08 Jul 2025	Whuups Inc. sends a formal IP theft and code infringement notice to GitHub with request for takedown and seizure of NSL repositories.

5

Annexure B – Payment Chart (PayPal Transactions)

Vendor: NSL Infotech Pvt. Ltd.

Total Amount Paid: $30,823.71 USD

Dayment mode: PayPal

Date	Amount (USD)	Transaction ID / Bill ID
03/11/2024	$500.00	3RR82478B77762948
04/11/2024	$948.00	17E527498N931142H
05/11/2024	$792.00	5WB39870CV376112R
06/11/2024	$3,000.00	7SH84339J7796791L
13/11/2024	$1,500.00	7N217646Y39885633
29/11/2024	$500.00	0X95940098929840G
13/12/2024	$1,424.00	U-6DN05218GY8604825
04/02/2025	$195.00	6PL09061U6884571N / U-8LP44886BR732091S
12/02/2025	$1,200.00	4A6804047A9741401 / U-5D1580335S328615M
12/02/2025	$1,040.00	7JW262226K207034M / U-43E33239KD6574529
12/02/2025	$1,619.00	7D656193CV867935W / U-4YU71808S05121225
06/03/2025	$1,055.00	2EF32895AR870282R / U-2DA234555F563343F
06/03/2025	$3,000.00	9W008381S1888234W
06/03/2025	$200.00	9FJ741800S080245T
07/03/2025	$700.00	6LW25596PT634351D
03/04/2025	$1,500.00	4017014244734622H
03/04/2025	$1,448.71	0EM617971D297043N
22/05/2025	$5,000.00	45175250F1779722N
04/06/2025	$2,800.00	70U93687TU3660527

Total Amount Paid by whuups inc.: $30,823.71 USD

GitHub Security Violation – Final Statement

Incident Summary:

- On **March 17, 2025**, Gaurav Sethi created an unauthorized backup GitHub key without any consent or authorization.
- Using this key, he **illegally accessed our private repositories** (hacking), **downloaded the full source code**(intellectual property theft), and tampered with repository permissions, blocking our team from accessing our own code.
- Gaurav **admitted to removing our code access** while retaining a local copy of the entire repository, which constitutes **intellectual property theft, hacking, and malicious tampering**.
- **All his access was discovered and completely revoked on July 25, 2025**, two days ago, following a full security audit.

Illegal Activities Identified

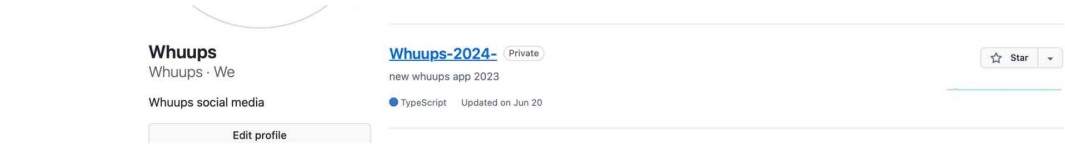
1. **Unauthorized GitHub Access (Hacking):** A clear violation of cybersecurity laws.
2. **Downloading Proprietary Code (Intellectual Property Theft):** Stealing company-owned source code.
3. **Removal of Authorized Team Access (Sabotage):** Preventing rightful owners from maintaining their own repository.
4. **Continued Unauthorized Attempts:** Evidence shows further login attempts on **June 21, 2025**, after access was revoked.

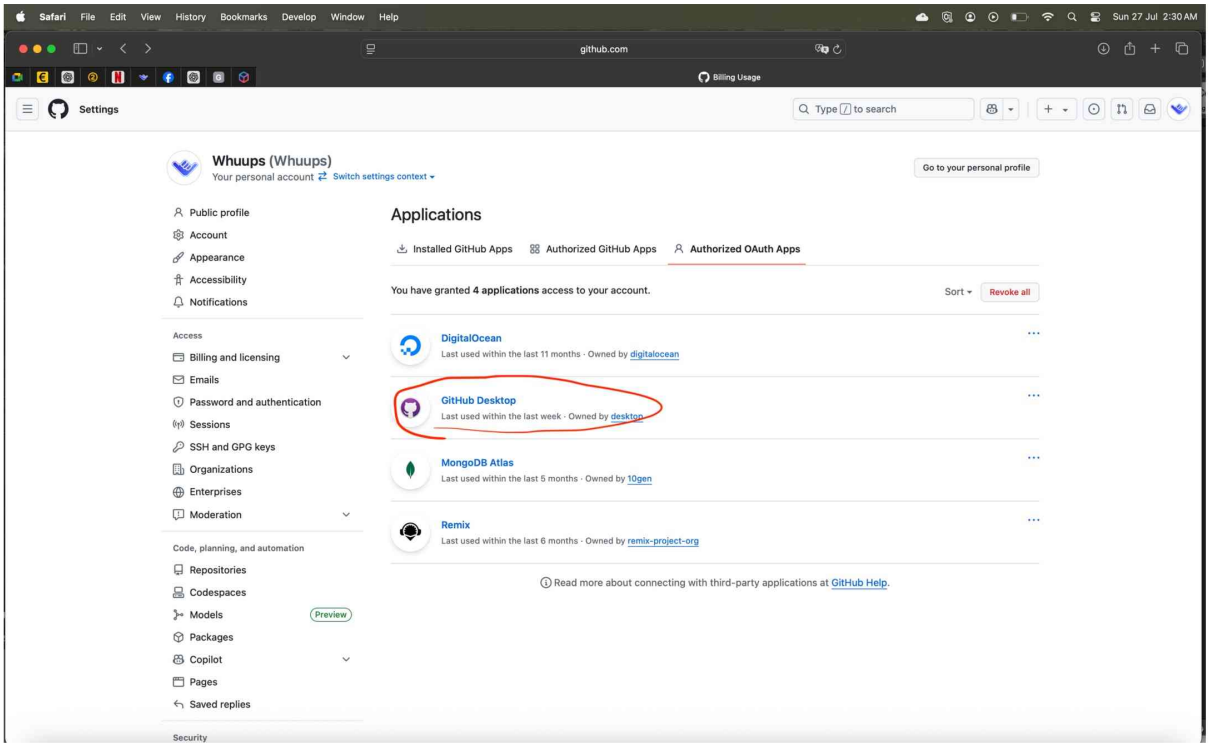
Legal and Security Actions

- **All GitHub keys created by Gaurav Sethi are permanently revoked** as of **July 25, 2025**.
- We have **documented all logs, admissions, and activities** for legal and compliance purposes.
- **2FA and strict key rotation policies** have been implemented on all repositories.
- Legal proceedings will treat these acts as **criminal hacking, intellectual property theft, and sabotage**.

https://docs.github.com/en/authentication/securing-your-account-with-two-factor-authentication-2fa/accessing-github-using-two-factor-authentication#verifying-with-github-mobile

NSL-Infotech-PVT-LTD/whuups-mobile-app

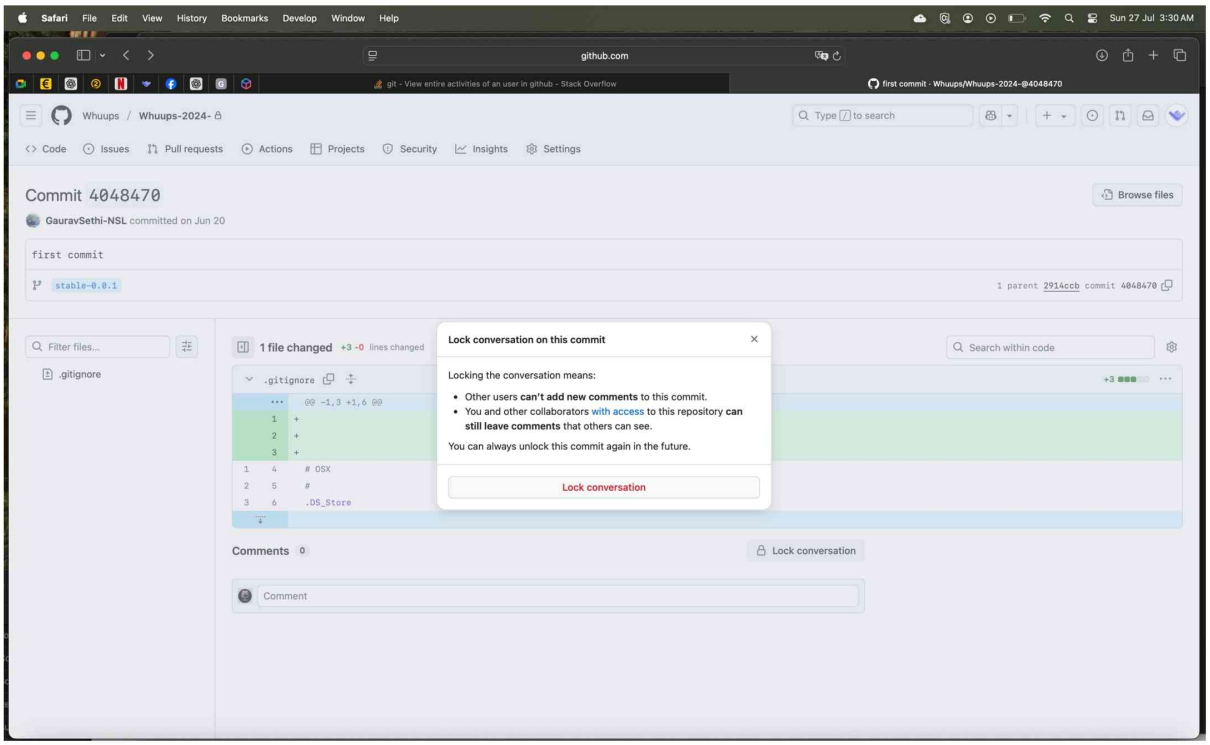


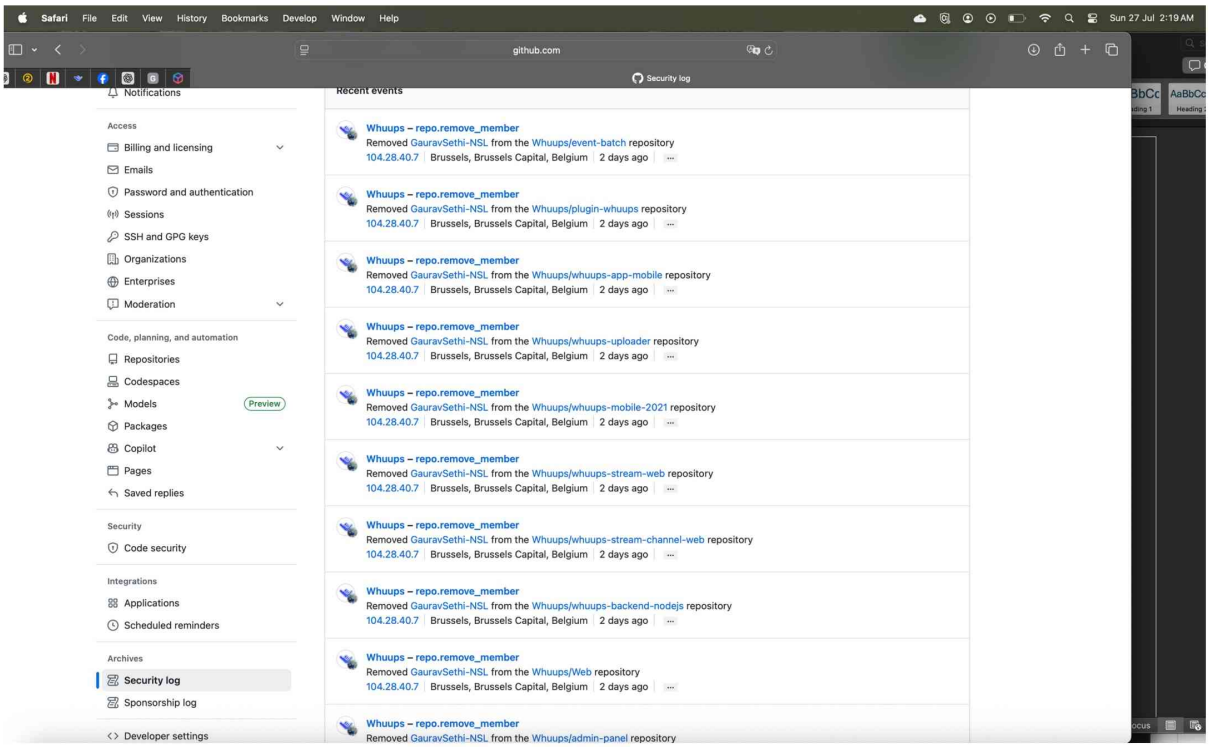


NSL-Infotech-PVT-LTD – repo.remove_member
Removed Whuups from the NSL-Infotech-PVT-LTD/whuups-mobile-app repository
on Jun 23 ...

@timestamp	2025-06-23 08:55:22 -0400
_document_id	EgbpNRsSJdwFUowJ61W7GA
action	repo.remove_member
actor	NSL-Infotech-PVT-LTD
actor_id	91871648
actor_is_bot	false
created_at	2025-06-23 08:55:22 -0400
operation_type	remove
org	NSL-Infotech-PVT-LTD
org_id	91871648
public_repo	false
repo	NSL-Infotech-PVT-LTD/whuups-mobile-app
repo_id	969478679
request_access_security_header	*nil*
request_id	CE40:2F5B2B:A6FF19:C62ED0:68594EB5
user	Whuups
user_agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/...
user_id	72411461
visibility	private

Newer Older


Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 3:30 AM
github.com
git - View entire activities of an user in github - Stack Overflow
first commit · Whuups/Whuups-2024-@4048470
Whuups / Whuups-2024-
Type / to search
Code Issues Pull requests Actions Projects Security Insights Settings
Commit 4048470
Browse files
GauravSethi-NSL committed on Jun 20
first commit
stable-0.0.1
1 parent 2914ccb commit 4048470
Filter files...
.gitignore
1 file changed +3 -0 lines changed
Search within code
Lock conversation on this commit
Locking the conversation means:
Other users can't add new comments to this commit.
You and other collaborators with access to this repository can still leave comments that others can see.
You can always unlock this commit again in the future.
Lock conversation
.gitignore
@@ -1,3 +1,6 @@
1 +
2 +
3 +
1 4 # OSX
2 5 #
3 6 .DS_Store
Comments 0
Lock conversation
Comment



device. For more information, see Recovering your account if you lose your 2FA credentials.

In this artic

Performing
Using two-f
Troublesho
Further rea

Using a security key

If you've set up a security key on your account, and your browser supports security keys, you can use it to complete your sign in.

1. Using your username and password, sign in to GitHub through your browser.
2. If you use a physical security key, ensure it's connected to your device.
3. To trigger the security key prompt from your operating system, select "Use security key."
4. Select the appropriate option in the prompt. Depending on your security key configuration, you may type a PIN, complete a biometric prompt, or use a physical security key.

Using a passkey

If you have enabled 2FA, and you have added a passkey to your account, you can use the passkey to sign in. Since passkeys satisfy both password and 2FA requirements, you can complete your sign in with a single step. See About passkeys.

Receiving a text message

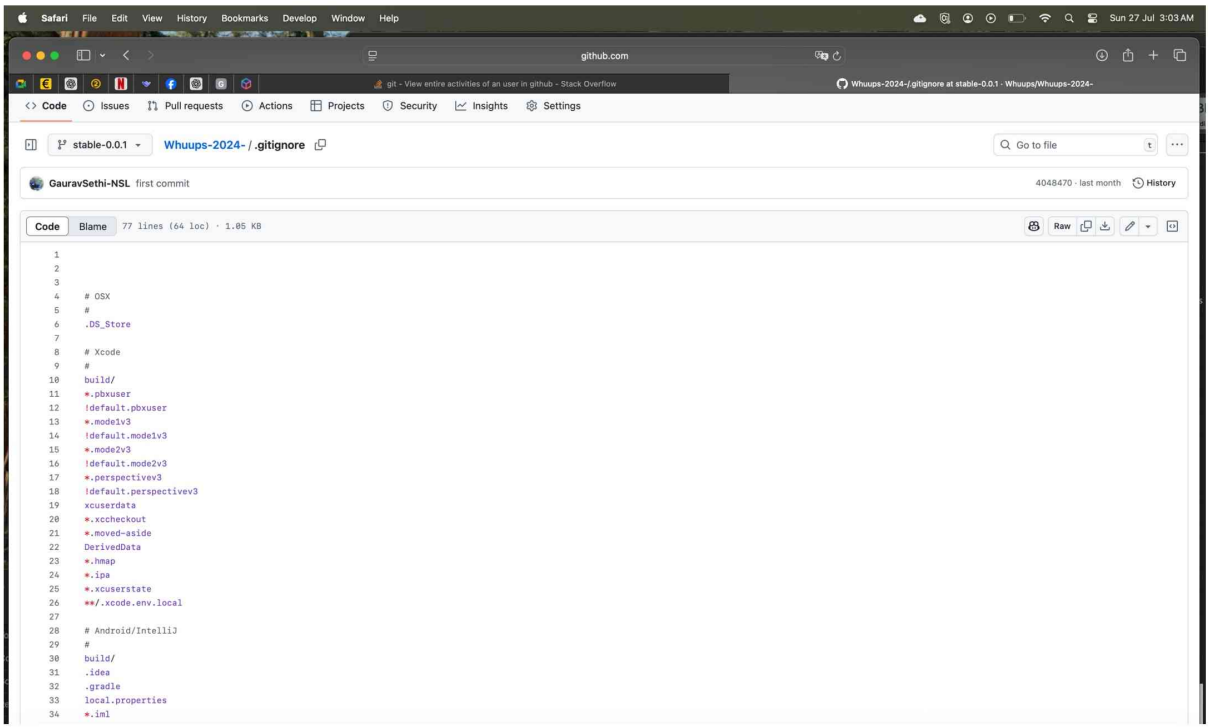
If you set up two-factor authentication via text messages, GitHub will send you a text message with your authentication code.

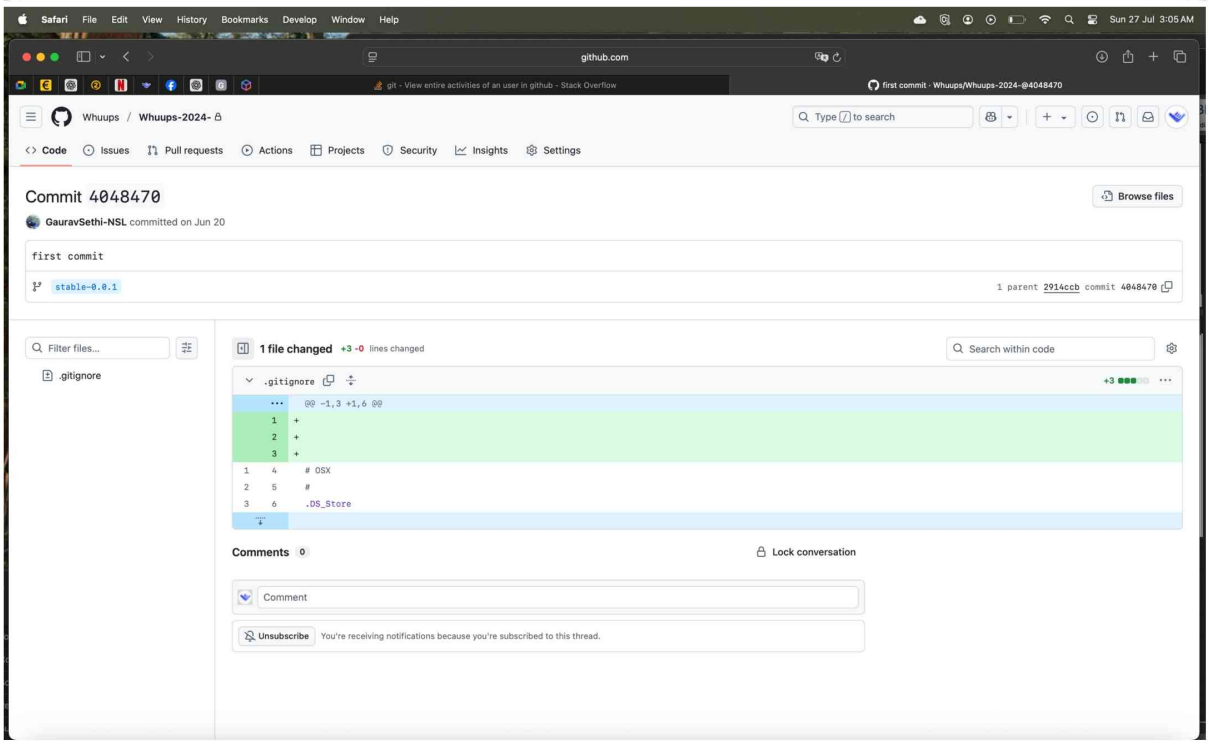
Verifying with GitHub Mobile

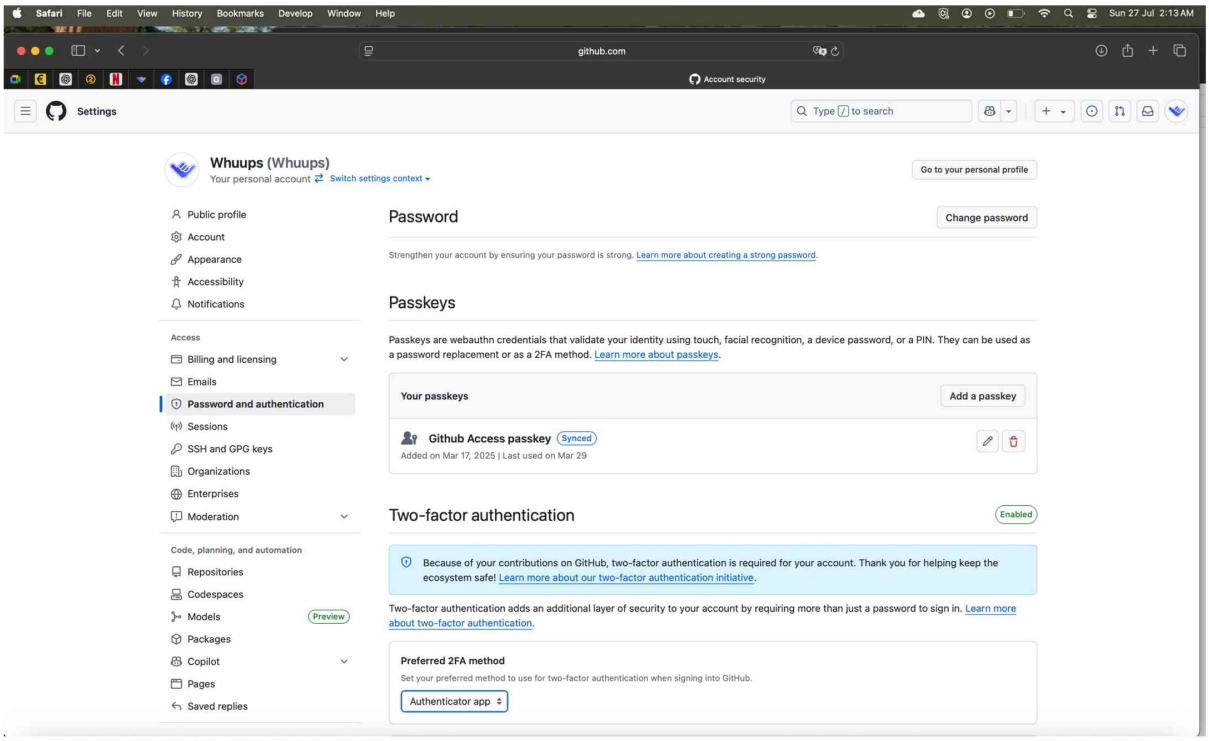
If you have installed and signed in to GitHub Mobile, you may choose to authenticate with GitHub Mobile for two-factor authentication.

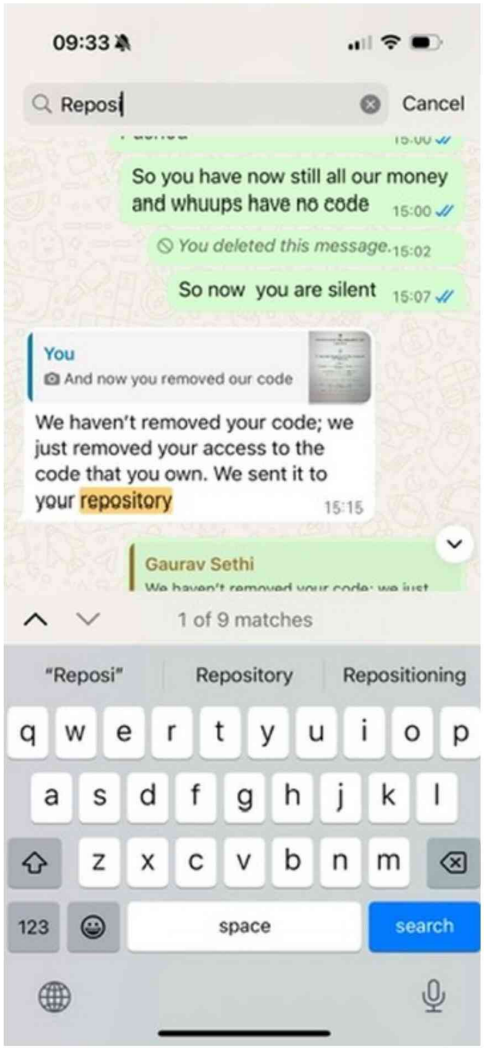
1. Sign in to GitHub with your browser, using your username and password.
2. GitHub will send you a push notification to verify your sign in attempt. Opening the push notification or opening the GitHub Mobile app will display a prompt, asking you to approve or

Microsoft Pow


Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 3:03 AM
github.com
Whuups-2024-/.gitignore at stable-0.0.1 · Whuups/Whuups-2024-
Code Issues Pull requests Actions Projects Security Insights Settings
stable-0.0.1 Whuups-2024- / .gitignore
Go to file
GauravSethi-NSL first commit
4048470 · last month History
Code Blame 77 lines (64 loc) · 1.05 KB
Raw
OSX
#
.DS_Store
Xcode
#
build/
*.pbxuser
!default.pbxuser
*.mode1v3
!default.mode1v3
*.mode2v3
!default.mode2v3
*.perspectivev3
!default.perspectivev3
xcuserdata
*.xccheckout
*.moved-aside
DerivedData
*.hmap
*.ipa
*.xcuserstate
**/.xcode.env.local
Android/IntelliJ
#
build/
.idea
.gradle
local.properties
*.iml


Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 3:05 AM
github.com
first commit · Whuups/Whuups-2024-@4048470
Whuups / Whuups-2024-
Type / to search
Code Issues Pull requests Actions Projects Security Insights Settings
Commit 4048470
Browse files
GauravSethi-NSL committed on Jun 20
first commit
stable-0.0.1
1 parent 2914ccb commit 4048470
Filter files...
.gitignore
1 file changed +3 -0 lines changed
Search within code
.gitignore
@@ -1,3 +1,6 @@
+
+
+
OSX
#
.DS_Store
Comments 0
Lock conversation
Comment
Unsubscribe
You're receiving notifications because you're subscribed to this thread.


Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 2:13 AM
github.com
Account security
Settings
Type / to search
Whuups (Whuups)
Your personal account
Switch settings context
Go to your personal profile
Public profile
Account
Appearance
Accessibility
Notifications
Access
Billing and licensing
Emails
Password and authentication
Sessions
SSH and GPG keys
Organizations
Enterprises
Moderation
Code, planning, and automation
Repositories
Codespaces
Models
Preview
Packages
Copilot
Pages
Saved replies
Password
Change password
Strengthen your account by ensuring your password is strong. Learn more about creating a strong password.
Passkeys
Passkeys are webauthn credentials that validate your identity using touch, facial recognition, a device password, or a PIN. They can be used as a password replacement or as a 2FA method. Learn more about passkeys.
Your passkeys
Add a passkey
Github Access passkey
Synced
Added on Mar 17, 2025 | Last used on Mar 29
Two-factor authentication
Enabled
Because of your contributions on GitHub, two-factor authentication is required for your account. Thank you for helping keep the ecosystem safe! Learn more about our two-factor authentication initiative.
Two-factor authentication adds an additional layer of security to your account by requiring more than just a password to sign in. Learn more about two-factor authentication.
Preferred 2FA method
Set your preferred method to use for two-factor authentication when signing into GitHub.
Authenticator app


09:33
Reposi
Cancel
So you have now still all our money and whuups have no code 15:00
You deleted this message. 15:02
So now you are silent 15:07
You
And now you removed our code
We haven't removed your code; we just removed your access to the code that you own. We sent it to your repository 15:15
Gaurav Sethi
1 of 9 matches
"Reposi"
Repository
Repositioning
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
search

1. Evidence of Unauthorized AWS Access

Key Account Identified

- **User/Email:** `server.operations@netscapelabs.com`
- **ARN:** `arn:aws:iam::491085412805:user/server.operations@netscapelabs.com`
- **Platform:** AWS IAM (Identity and Access Management)

This account (`server.operations@netscapelabs.com`) shows signs of **unauthorized access** to the Whuups AWS platform. The claim is that all legitimate access was removed, but new credentials were **illegally created and used**.

---

2. Timeline of Access

June 21, 2025 (Initial Unauthorized Access)

- You allege that **Sethi** accessed the AWS platform **without authorization** on June 21, 2025.
- This would typically be verified by **AWS CloudTrail logs**, which record all login attempts and API actions.

Evidence to collect here:

- CloudTrail logs showing `ConsoleLogin` or `AssumeRole` events for `server.operations@netscapelabs.com`.
- The source IP address used during the login attempt (to prove external, unauthorized activity).

June 29, 2025 (Your Notification)

- According to your note, after your letter dated **June 29, 2025**, you removed NSL's access.
- However, NSL allegedly **created a new IAM user or access key**, which is a clear violation.

July 1, 2025 (New Keys Created)

- You mention that **on July 1**, new **access keys were created**.
- This is strong evidence of unauthorized activity because **only an AWS Admin should be able to create keys**.

Evidence to collect here:

- CloudTrail `CreateAccessKey` events.
- IAM `AccessKeyLastUsed` data (which shows the exact time and services accessed).
- Any `PutUserPolicy` or `AttachUserPolicy` logs (indicating attempts to modify permissions).

Access 3 Hours Ago (Latest Intrusion)

- The mention of **"access 3 hours ago"** suggests **ongoing unauthorized activity**, even after revoking keys.
- This could indicate:
  - **A backdoor IAM user** created earlier that was not removed.
  - **AWS CLI or API calls** made from an already issued access key.

Evidence to collect here:

- CloudTrail events from the last 3-6 hours.
- IAM `ListUsers` and `ListAccessKeys` outputs to confirm no hidden users or keys remain.
- AWS GuardDuty findings (if enabled).

---

3. What This Evidence Proves

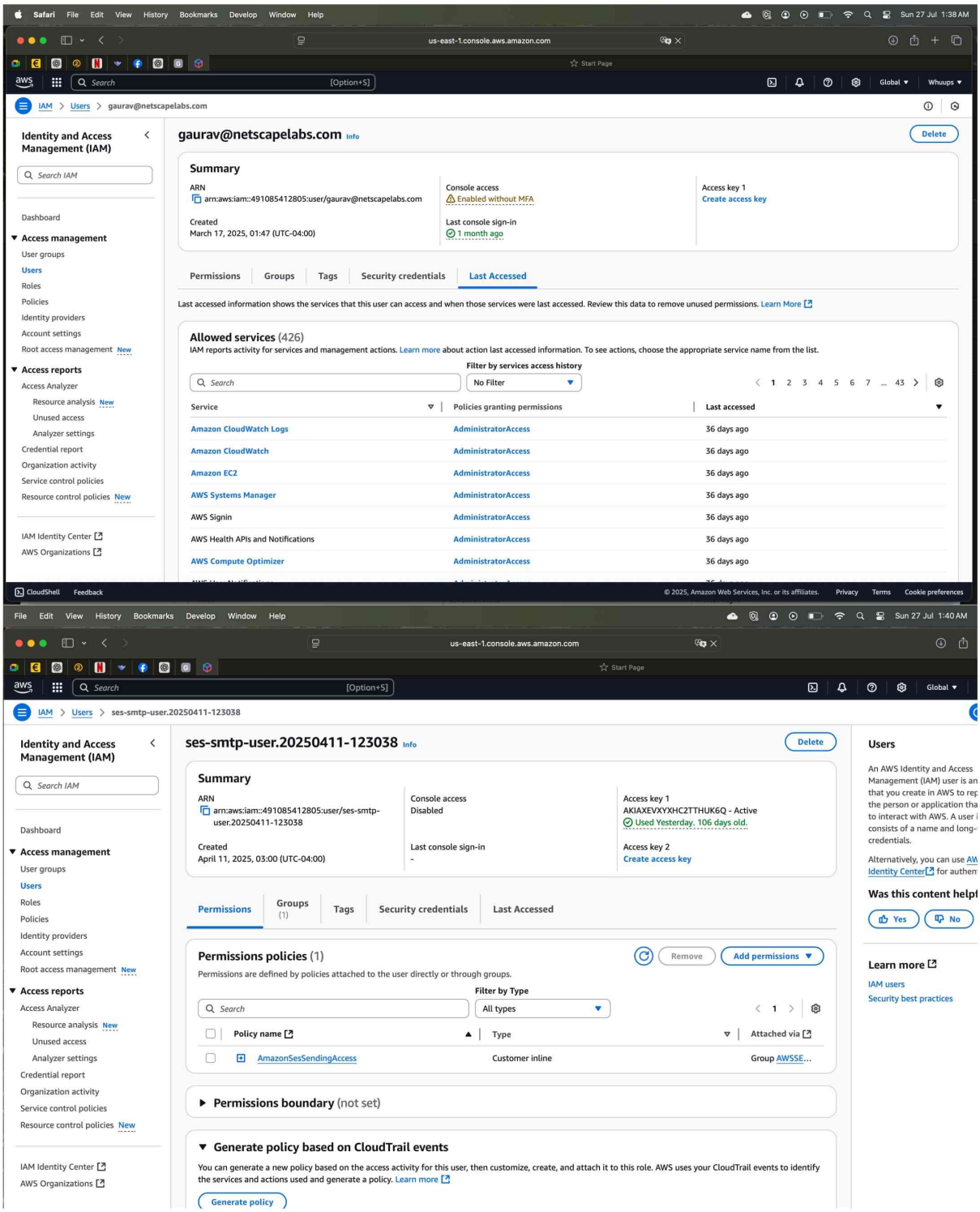
- The pattern of events indicates that **unauthorized users** (likely from NSL or acting under Sethi) are still able to **create keys and log in**.
- Since the **access was removed**, but **new accounts or keys keep appearing**, it implies **fraudulent and malicious actions** (possibly exploiting old root credentials or compromised IAM roles).

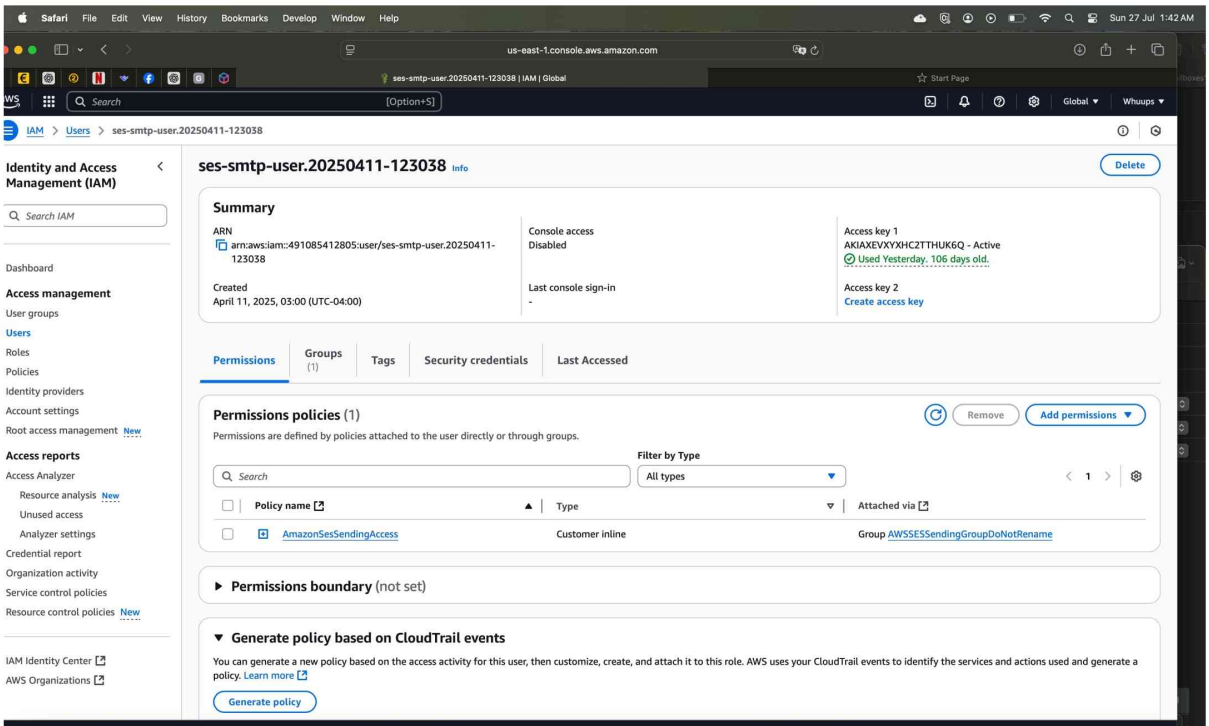
---

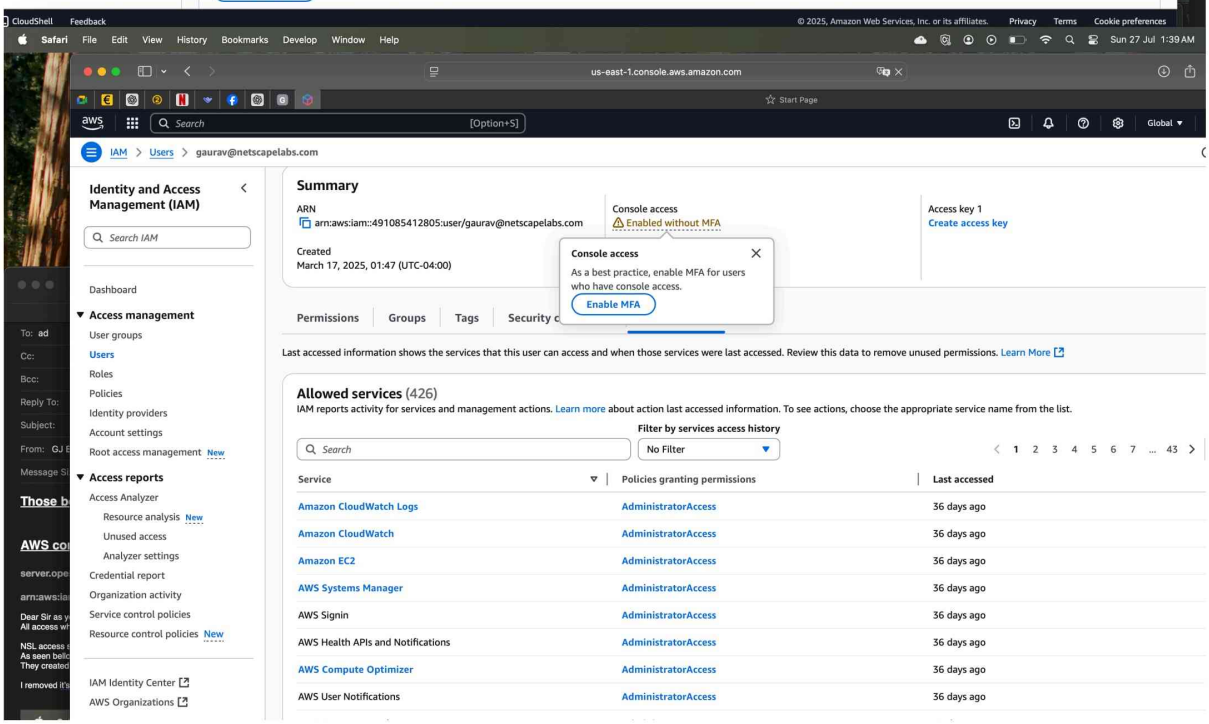
4. Steps to Strengthen the Case

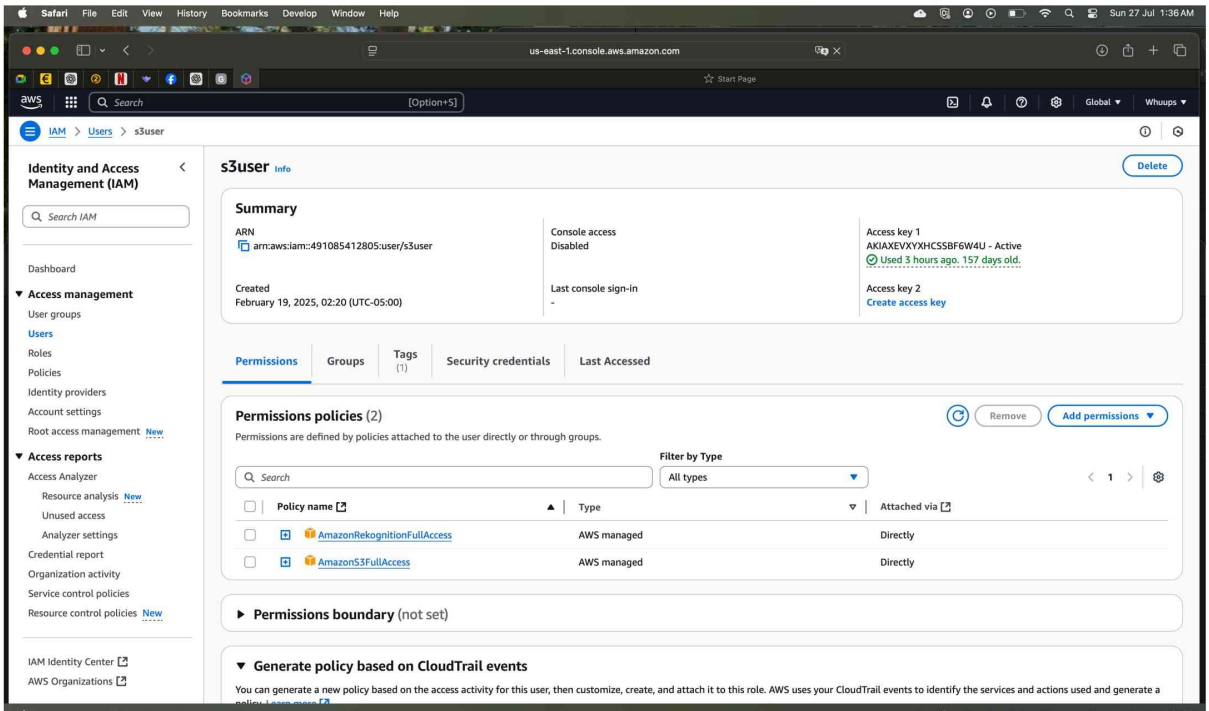
To present this evidence formally, you should:

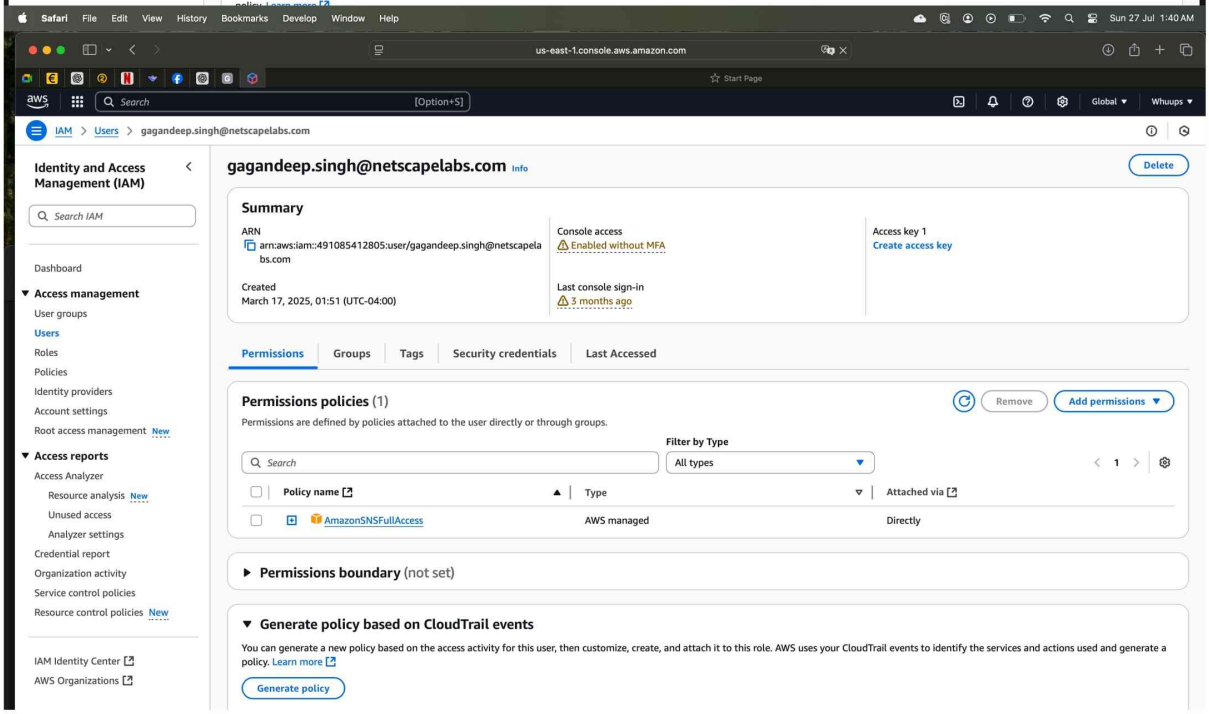
1. **Export CloudTrail logs** (CSV or JSON) for:
   - `ConsoleLogin`, `CreateAccessKey`, `GenerateServiceLastAccessedDetails`, and `DeleteAccessKey`.
2. **Document all timestamps** of unauthorized logins (e.g., June 21, July 1, and 3 hours ago).
3. **Take screenshots** of AWS IAM users, roles, and keys (showing the creation dates).
4. **Enable MFA and rotate root credentials** immediately to prevent further abuse.

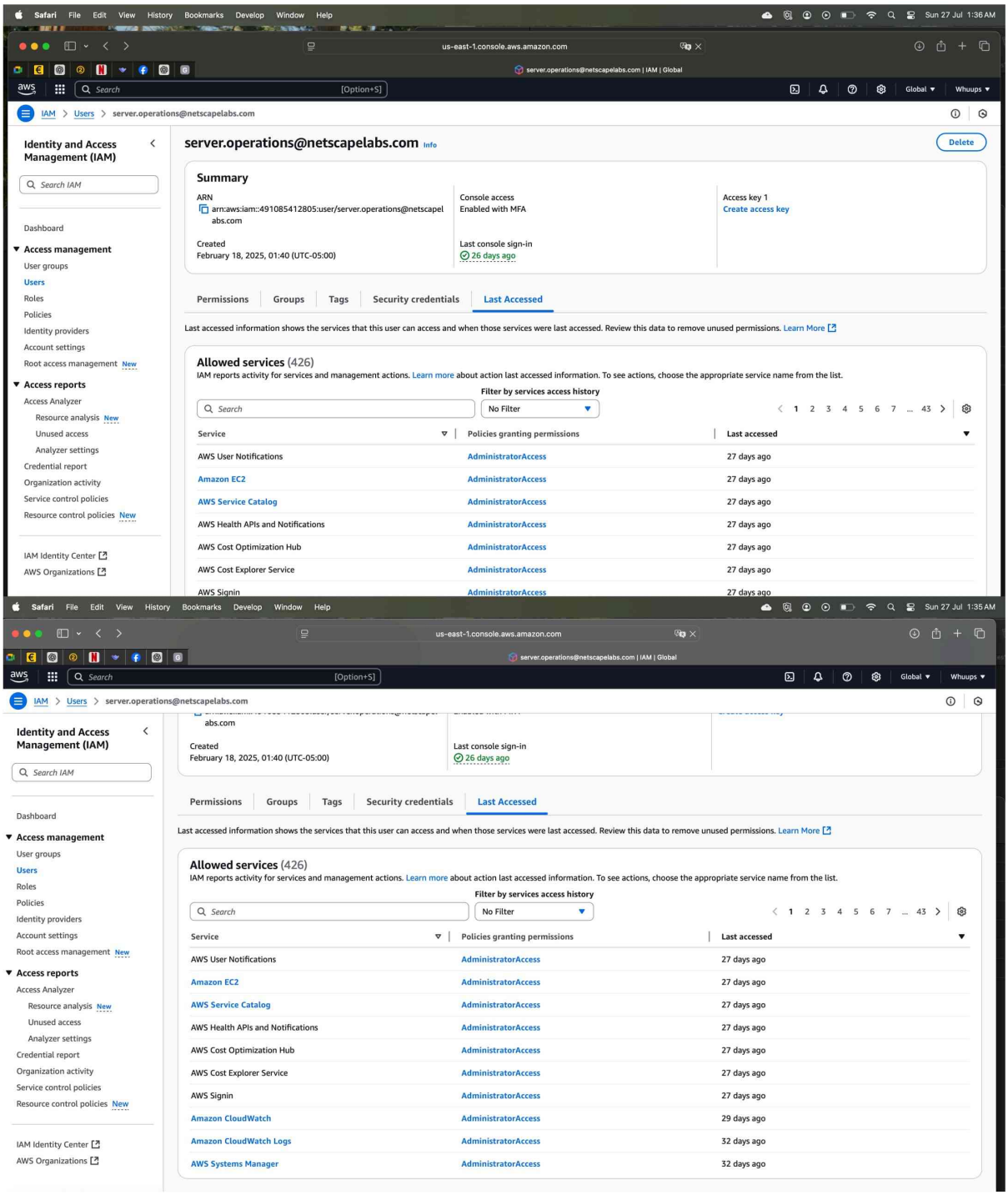

Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:38 AM
us-east-1.console.aws.amazon.com
Start Page
Search [Option+S]
Global
Whuups
IAM > Users > gaurav@netscapelabs.com
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
gaurav@netscapelabs.com Info
Delete
Summary
ARN
arn:aws:iam::491085412805:user/gaurav@netscapelabs.com
Console access
Enabled without MFA
Access key 1
Create access key
Created
March 17, 2025, 01:47 (UTC-04:00)
Last console sign-in
1 month ago
Permissions
Groups
Tags
Security credentials
Last Accessed
Last accessed information shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. Learn More
Allowed services (426)
IAM reports activity for services and management actions. Learn more about action last accessed information. To see actions, choose the appropriate service name from the list.
Filter by services access history
Search
No Filter
1 2 3 4 5 6 7 ... 43
Service
Policies granting permissions
Last accessed
Amazon CloudWatch Logs AdministratorAccess 36 days ago
Amazon CloudWatch AdministratorAccess 36 days ago
Amazon EC2 AdministratorAccess 36 days ago
AWS Systems Manager AdministratorAccess 36 days ago
AWS Signin AdministratorAccess 36 days ago
AWS Health APIs and Notifications AdministratorAccess 36 days ago
AWS Compute Optimizer AdministratorAccess 36 days ago
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:40 AM
us-east-1.console.aws.amazon.com
Start Page
Search [Option+S]
Global
IAM > Users > ses-smtp-user.20250411-123038
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
ses-smtp-user.20250411-123038 Info
Delete
Summary
ARN
arn:aws:iam::491085412805:user/ses-smtp-user.20250411-123038
Console access
Disabled
Access key 1
AKIAXEVXYXHC2TTHUK6Q - Active
Used Yesterday. 106 days old.
Created
April 11, 2025, 03:00 (UTC-04:00)
Last console sign-in
-
Access key 2
Create access key
Permissions
Groups (1)
Tags
Security credentials
Last Accessed
Permissions policies (1)
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
AmazonSesSendingAccess Customer inline Group AWSSE...
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy
Users
An AWS Identity and Access Management (IAM) user is an
that you create in AWS to rep
the person or application tha
to interact with AWS. A user
consists of a name and long-
credentials.
Alternatively, you can use AW
Identity Center for authen
Was this content helpf
Yes
No
Learn more
IAM users
Security best practices

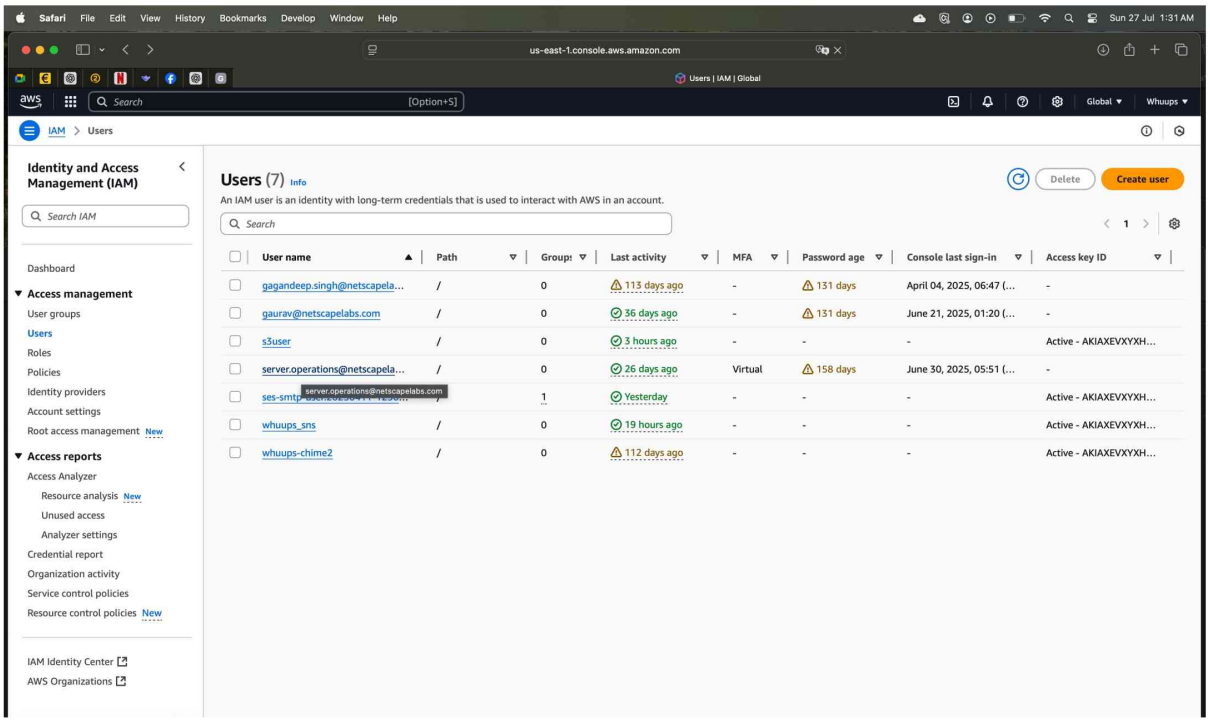

Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:42 AM
us-east-1.console.aws.amazon.com
ses-smtp-user.20250411-123038 | IAM | Global
Start Page
Search [Option+S]
Global
Whuups
IAM > Users > ses-smtp-user.20250411-123038
Identity and Access Management (IAM)
Search IAM
Dashboard
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
ses-smtp-user.20250411-123038 Info
Delete
Summary
ARN
arn:aws:iam::491085412805:user/ses-smtp-user.20250411-123038
Created
April 11, 2025, 03:00 (UTC-04:00)
Console access
Disabled
Last console sign-in
-
Access key 1
AKIAXEVXYXHC2TTHUK6Q - Active
Used Yesterday. 106 days old.
Access key 2
Create access key
Permissions
Groups (1)
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Search
Filter by Type
All types
Policy name
Type
Attached via
AmazonSesSendingAccess
Customer inline
Group AWSSESSendingGroupDoNotRename
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

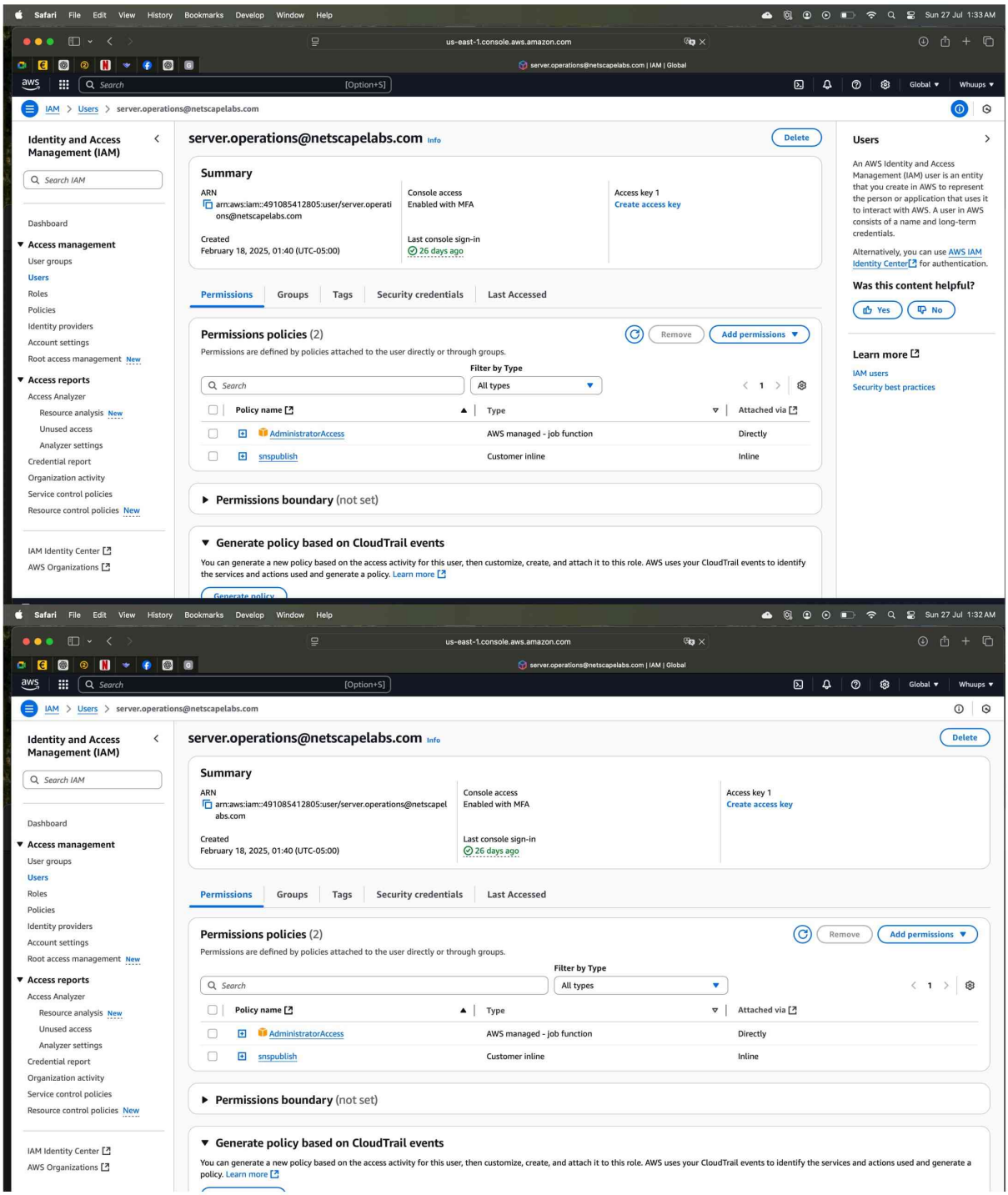

Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:39 AM
us-east-1.console.aws.amazon.com
Start Page
Search [Option+S]
Global
IAM > Users > gaurav@netscapelabs.com
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Summary
ARN
arn:aws:iam::491085412805:user/gaurav@netscapelabs.com
Created
March 17, 2025, 01:47 (UTC-04:00)
Console access
Enabled without MFA
Console access
As a best practice, enable MFA for users who have console access.
Enable MFA
Access key 1
Create access key
Permissions
Groups
Tags
Last accessed information shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. Learn More
Allowed services (426)
IAM reports activity for services and management actions. Learn more about action last accessed information. To see actions, choose the appropriate service name from the list.
Filter by services access history
Search
No Filter
1 2 3 4 5 6 7 ... 43
Service
Policies granting permissions
Last accessed
Amazon CloudWatch Logs AdministratorAccess 36 days ago
Amazon CloudWatch AdministratorAccess 36 days ago
Amazon EC2 AdministratorAccess 36 days ago
AWS Systems Manager AdministratorAccess 36 days ago
AWS Signin AdministratorAccess 36 days ago
AWS Health APIs and Notifications AdministratorAccess 36 days ago
AWS Compute Optimizer AdministratorAccess 36 days ago
AWS User Notifications AdministratorAccess 36 days ago


Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:36 AM
us-east-1.console.aws.amazon.com
Start Page
Search [Option+S]
Global
Whuups
IAM > Users > s3user
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
s3user Info
Delete
Summary
ARN
arn:aws:iam::491085412805:user/s3user
Console access
Disabled
Access key 1
AKIAXEVXYXHCSSBF6W4U - Active
Used 3 hours ago. 157 days old.
Created
February 19, 2025, 02:20 (UTC-05:00)
Last console sign-in
-
Access key 2
Create access key
Permissions
Groups
Tags (1)
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
Policy name
Type
Attached via
AmazonRekognitionFullAccess
AWS managed
Directly
AmazonS3FullAccess
AWS managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a

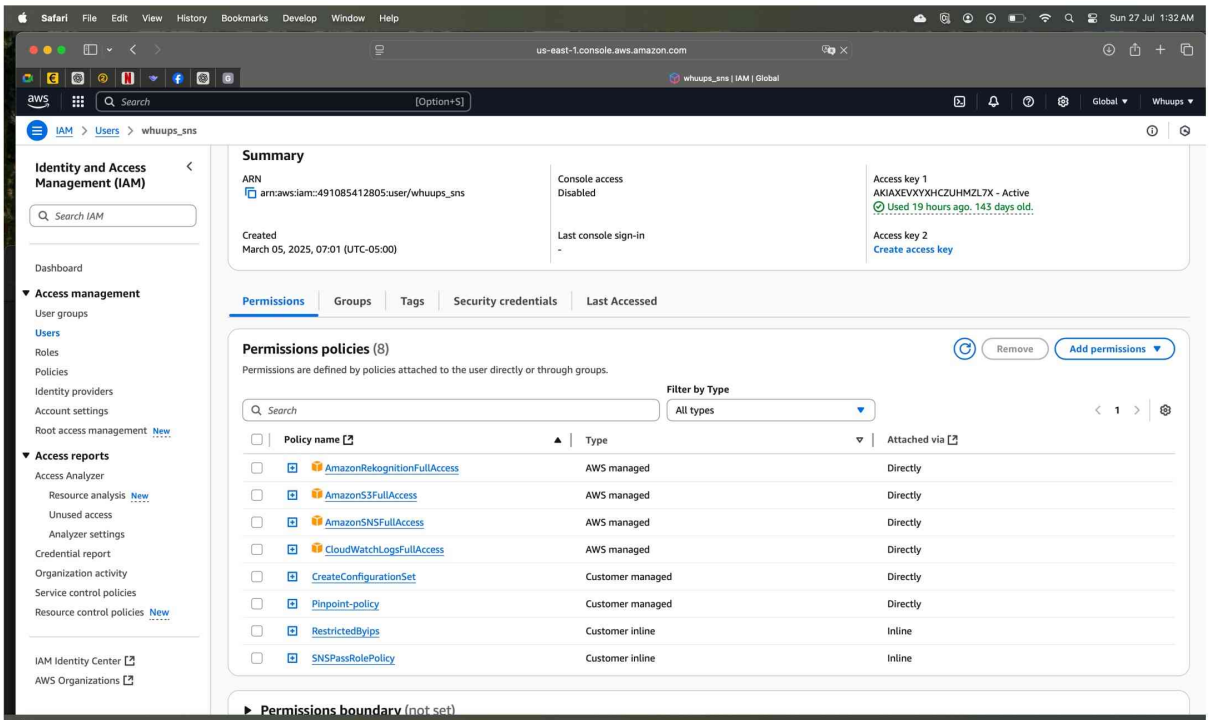

Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:40 AM
us-east-1.console.aws.amazon.com
Start Page
Search [Option+S]
Global
Whuups
IAM > Users > gagandeep.singh@netscapelabs.com
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
gagandeep.singh@netscapelabs.com Info
Delete
Summary
ARN
arn:aws:iam::491085412805:user/gagandeep.singh@netscapelabs.com
Console access
Enabled without MFA
Access key 1
Create access key
Created
March 17, 2025, 01:51 (UTC-04:00)
Last console sign-in
3 months ago
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached via
AmazonSNSFullAccess
AWS managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy

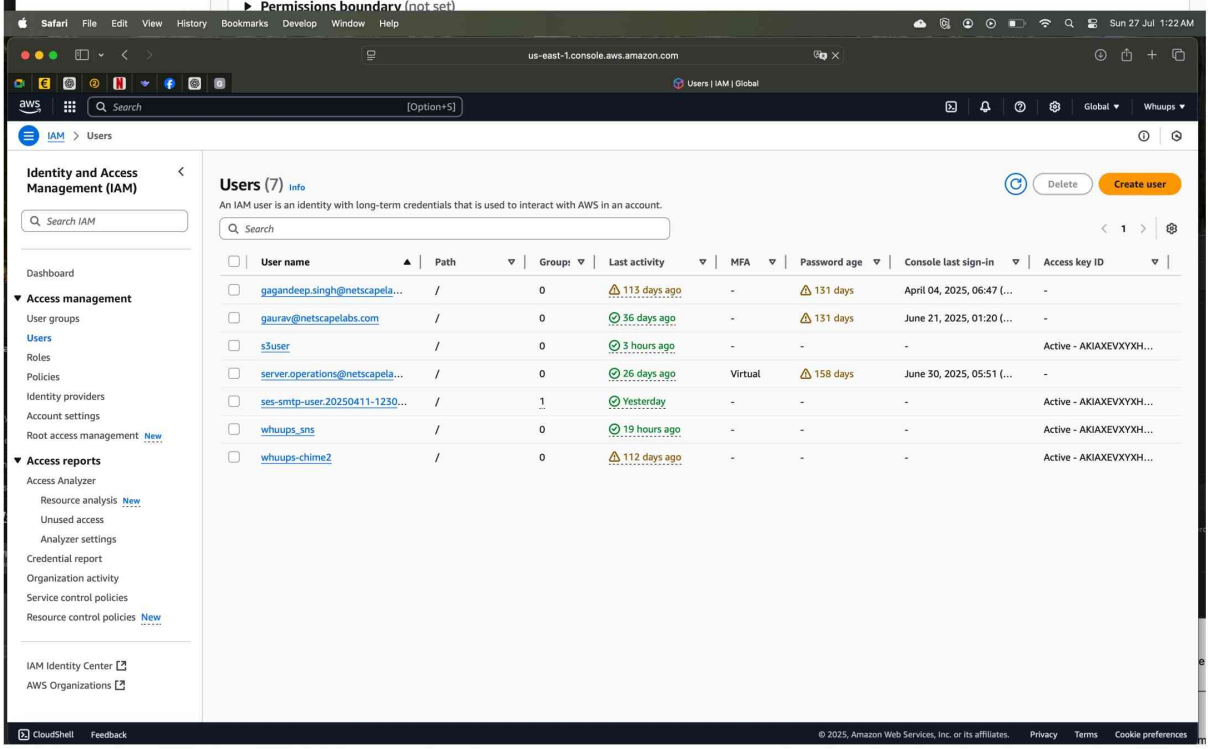

Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:36 AM
us-east-1.console.aws.amazon.com
server.operations@netscapelabs.com | IAM | Global
Search [Option+S]
Global
Whuups
IAM > Users > server.operations@netscapelabs.com
Identity and Access Management (IAM)
Search IAM
Dashboard
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
server.operations@netscapelabs.com Info
Delete
Summary
ARN
arn:aws:iam::491085412805:user/server.operations@netscapelabs.com
Console access
Enabled with MFA
Access key 1
Create access key
Created
February 18, 2025, 01:40 (UTC-05:00)
Last console sign-in
26 days ago
Permissions
Groups
Tags
Security credentials
Last Accessed
Last accessed information shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. Learn More
Allowed services (426)
IAM reports activity for services and management actions. Learn more about action last accessed information. To see actions, choose the appropriate service name from the list.
Filter by services access history
Search
No Filter
1 2 3 4 5 6 7 ... 43
Service
Policies granting permissions
Last accessed
AWS User Notifications AdministratorAccess 27 days ago
Amazon EC2 AdministratorAccess 27 days ago
AWS Service Catalog AdministratorAccess 27 days ago
AWS Health APIs and Notifications AdministratorAccess 27 days ago
AWS Cost Optimization Hub AdministratorAccess 27 days ago
AWS Cost Explorer Service AdministratorAccess 27 days ago
AWS Signin AdministratorAccess 27 days ago
Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:35 AM
us-east-1.console.aws.amazon.com
server.operations@netscapelabs.com | IAM | Global
Search [Option+S]
Global
Whuups
IAM > Users > server.operations@netscapelabs.com
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
abs.com
Created
February 18, 2025, 01:40 (UTC-05:00)
Last console sign-in
26 days ago
Permissions
Groups
Tags
Security credentials
Last Accessed
Last accessed information shows the services that this user can access and when those services were last accessed. Review this data to remove unused permissions. Learn More
Allowed services (426)
IAM reports activity for services and management actions. Learn more about action last accessed information. To see actions, choose the appropriate service name from the list.
Filter by services access history
Search
No Filter
1 2 3 4 5 6 7 ... 43
Service
Policies granting permissions
Last accessed
AWS User Notifications AdministratorAccess 27 days ago
Amazon EC2 AdministratorAccess 27 days ago
AWS Service Catalog AdministratorAccess 27 days ago
AWS Health APIs and Notifications AdministratorAccess 27 days ago
AWS Cost Optimization Hub AdministratorAccess 27 days ago
AWS Cost Explorer Service AdministratorAccess 27 days ago
AWS Signin AdministratorAccess 27 days ago
Amazon CloudWatch AdministratorAccess 29 days ago
Amazon CloudWatch Logs AdministratorAccess 32 days ago
AWS Systems Manager AdministratorAccess 32 days ago

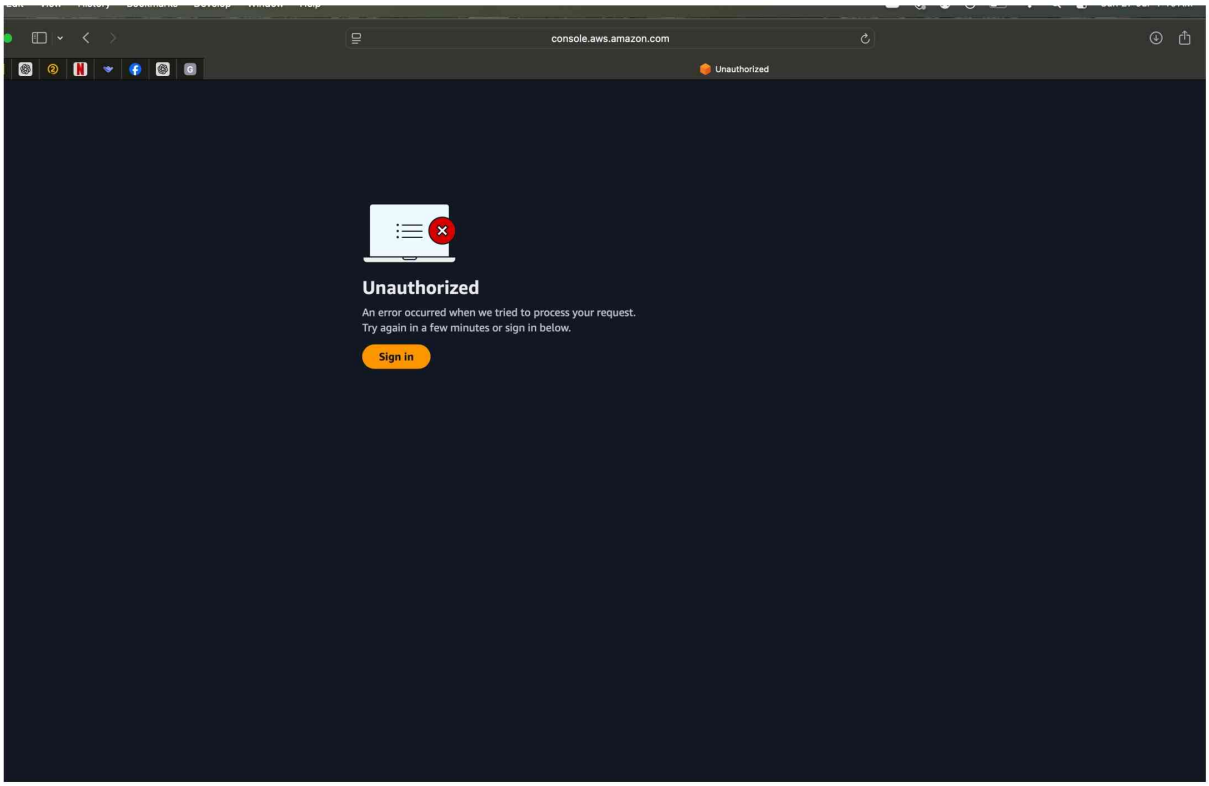

Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:31 AM
us-east-1.console.aws.amazon.com
Users | IAM | Global
Search [Option+S]
Global
Whuups
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Users (7) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search
Delete
Create user
1
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
Access key ID
gagandeep.singh@netscapela...
/
0
113 days ago
-
131 days
April 04, 2025, 06:47 (...
-
gaurav@netscapelabs.com
/
0
36 days ago
-
131 days
June 21, 2025, 01:20 (...
-
s3user
/
0
3 hours ago
-
-
-
Active - AKIAXEVXYXH...
server.operations@netscapela...
/
0
26 days ago
Virtual
158 days
June 30, 2025, 05:51 (...
-
server.operations@netscapelabs.com
ses-smtp
/
1
Yesterday
-
-
-
Active - AKIAXEVXYXH...
whuups_sns
/
0
19 hours ago
-
-
-
Active - AKIAXEVXYXH...
whuups-chime2
/
0
112 days ago
-
-
-
Active - AKIAXEVXYXH...


Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:33 AM
us-east-1.console.aws.amazon.com
server.operations@netscapelabs.com | IAM | Global
Search [Option+S]
Global
Whuups
IAM > Users > server.operations@netscapelabs.com
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
server.operations@netscapelabs.com Info
Delete
Summary
ARN
arn:aws:iam::491085412805:user/server.operations@netscapelabs.com
Console access
Enabled with MFA
Access key 1
Create access key
Created
February 18, 2025, 01:40 (UTC-05:00)
Last console sign-in
26 days ago
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
Policy name
Type
Attached via
AdministratorAccess
AWS managed - job function
Directly
snspublish
Customer inline
Inline
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Users
An AWS Identity and Access Management (IAM) user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user in AWS consists of a name and long-term credentials.
Alternatively, you can use AWS IAM Identity Center for authentication.
Was this content helpful?
Yes
No
Learn more
IAM users
Security best practices

Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:32 AM
us-east-1.console.aws.amazon.com
server.operations@netscapelabs.com | IAM | Global
Search [Option+S]
Global
Whuups
IAM > Users > server.operations@netscapelabs.com
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
server.operations@netscapelabs.com Info
Delete
Summary
ARN
arn:aws:iam::491085412805:user/server.operations@netscapelabs.com
Console access
Enabled with MFA
Access key 1
Create access key
Created
February 18, 2025, 01:40 (UTC-05:00)
Last console sign-in
26 days ago
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
Policy name
Type
Attached via
AdministratorAccess
AWS managed - job function
Directly
snspublish
Customer inline
Inline
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more


Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:32 AM
us-east-1.console.aws.amazon.com
whuups_sns | IAM | Global
Search [Option+S]
Global
Whuups
IAM > Users > whuups_sns
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Summary
ARN
arn:aws:iam::491085412805:user/whuups_sns
Console access
Disabled
Access key 1
AKIAXEVXYXHCZUHMZL7X - Active
Used 19 hours ago. 143 days old.
Created
March 05, 2025, 07:01 (UTC-05:00)
Last console sign-in
-
Access key 2
Create access key
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (8)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Search
Filter by Type
All types
Policy name
Type
Attached via
AmazonRekognitionFullAccess
AWS managed
Directly
AmazonS3FullAccess
AWS managed
Directly
AmazonSNSFullAccess
AWS managed
Directly
CloudWatchLogsFullAccess
AWS managed
Directly
CreateConfigurationSet
Customer managed
Directly
Pinpoint-policy
Customer managed
Directly
RestrictedByips
Customer inline
Inline
SNSPassRolePolicy
Customer inline
Inline
Permissions boundary (not set)


Safari File Edit View History Bookmarks Develop Window Help
Sun 27 Jul 1:22 AM
us-east-1.console.aws.amazon.com
Users | IAM | Global
Search [Option+S]
Global
Whuups
IAM > Users
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
Credential report
Organization activity
Service control policies
Resource control policies New
IAM Identity Center
AWS Organizations
Users (7) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
Access key ID
gagandeep.singh@netscapela...
/
0
113 days ago
-
131 days
April 04, 2025, 06:47 (...
-
gaurav@netscapelabs.com
/
0
36 days ago
-
131 days
June 21, 2025, 01:20 (...
-
s3user
/
0
3 hours ago
-
-
-
Active - AKIAXEVXYXH...
server.operations@netscapela...
/
0
26 days ago
Virtual
158 days
June 30, 2025, 05:51 (...
-
ses-smtp-user.20250411-1230...
/
1
Yesterday
-
-
-
Active - AKIAXEVXYXH...
whuups_sns
/
0
19 hours ago
-
-
-
Active - AKIAXEVXYXH...
whuups-chime2
/
0
112 days ago
-
-
-
Active - AKIAXEVXYXH...
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


console.aws.amazon.com
Unauthorized
Unauthorized
An error occurred when we tried to process your request.
Try again in a few minutes or sign in below.
Sign in

44.208.101.47 IP Address Profile

Whois | Diagnostics

IP Whois

```
Amazon.com, Inc. AMAZO-4 (NET-44-192-0-0-1) 44.192.0.0 - 44.255.255.255
Amazon Data Services NoVa AMAZON-IAD (NET-44-192-0-0-2) 44.192.0.0 - 44.223.255.255
```

controlpanel.whuups.com

WHOIS Information

Whois | RDAP | DNS Records | Uptime | Diagnostics | Hide Data | Refresh Data

WHOIS Lookup Results

No WHOIS data was found for **controlpanel.whuups.com**

This could be because:

- The domain doesn't exist
- The WHOIS server is temporarily unavailable
- The domain's registry doesn't provide WHOIS data

About WHOIS

WHOIS is a query and response protocol used for querying databases that store registered users of Internet resources, including domain names and IP addresses.

The protocol provides essential information about domain ownership, administrative contacts, and technical details that are invaluable for domain management and security purposes.

DNS Record Lookup

Look up DNS records including A, AAAA, MX, NS, SOA, and CNAME records for any domain

Enter a domain name... Search

controlpanel.whuups.com

DNS Records

Whois | RDAP | DNS Records | Uptime | Diagnostics | Hide Data

DNS Records for controlpanel.whuups.com

Hostname	Type	TTL	Priority	Content
controlpanel.whuups.com	A	0		44.208.101.47
controlpanel.whuups.com	A	0		52.5.48.230

44.208.101.47 IP Address Profile

Whois | Diagnostics

IP Whois

```
Amazon.com, Inc. AMAZO-4 (NET-44-192-0-0-1) 44.192.0.0 - 44.255.255.255
Amazon Data Services NoVa AMAZON-IAD (NET-44-192-0-0-2) 44.192.0.0 - 44.223.255.255
```

Enter a domain name... Search

controlpanel.whuups.com

Uptime & Server Information

Whois | RDAP | DNS Records | Uptime | Diagnostics | Hide Data

Current Status

Status	Inactive
Server Type	Unknown
Page Title	Not available
Meta Description	Not available
Meta Keywords	Not available
Most Recent Data	0 hours, 12 minutes ago

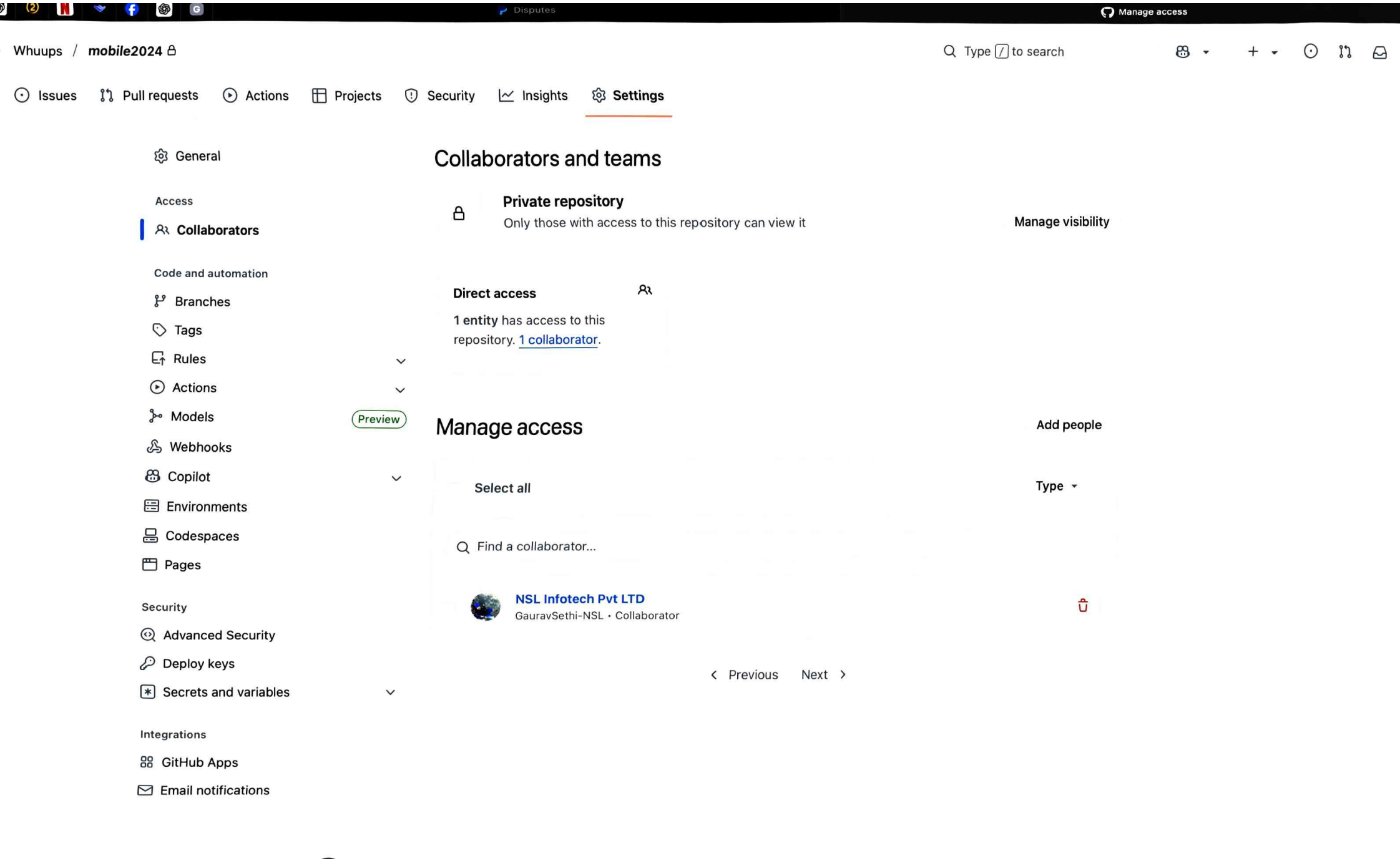
Historical Data

Date	Status	Server
7/27/2025, 4:55:42 AM	Inactive	Unknown

Traceroute Results

```
traceroute to 44.208.101.47 (44.208.101.47), 10 hops max, 60 byte packets
 1  ip-10-0-0-119.ec2.internal (10.0.0.119)  10.303 ms  10.264 ms  10.224 ms
 2  244.5.0.185 (244.5.0.185)  18.007 ms 244.5.0.159 (244.5.0.159)  10.512 ms 244.5.0.233
(244.5.0.233)  53.317 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  *
```

Results generated at: 27/07/2025, 00:57:19


Disputes
Manage access
Whuups / mobile2024
Type / to search
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
General
Access
Collaborators
Code and automation
Branches
Tags
Rules
Actions
Models
Preview
Webhooks
Copilot
Environments
Codespaces
Pages
Security
Advanced Security
Deploy keys
Secrets and variables
Integrations
GitHub Apps
Email notifications
Collaborators and teams
Private repository
Only those with access to this repository can view it
Manage visibility
Direct access
1 entity has access to this repository. 1 collaborator.
Manage access
Add people
Select all
Type
Find a collaborator...
NSL Infotech Pvt LTD
GauravSethi-NSL · Collaborator
Previous
Next

Disputes

GauravSethi-NSL (NSL Infotech Pvt LTD)

GauravSethi-NSL

Type / to search

Overview | Repositories | Projects | Packages | Stars 13

NSL Infotech Pvt LTD

GauravSethi-NSL

Follow

We seamlessly merge two key components – economics and information technology.

NSL Infotech PVT LTD

Chandigarh, INDIA

https://www.netscapelabs.com/

Block or Report

Popular repositories

GauravSethi-NSL doesn't have any public repositories yet.

0 contributions in the last year

2025

Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul

Mon

Wed

Fri

2024

2023

2022

2021

2020

Learn how we count contributions

Less More

Contribution activity

July 2025

GauravSethi-NSL has no activity yet for this period.

Show more activity

Whuups / **mobile2024**

Type / to search

Code | Issues | Pull requests | Actions | Projects | Security | Insights | **Settings**

- General

Access
- **Collaborators**

Code and automation
- Branches
- Tags
- Rules
- Actions
- Models — Preview
- Webhooks
- Copilot
- Environments
- Codespaces
- Pages

Security
- Advanced Security
- Deploy keys
- Secrets and variables

Integrations
- GitHub Apps
- Email notifications

Collaborators and teams

Private repository
Only those with access to this repository can view it

Manage visibility

Direct access

1 entity has access to this repository. 1 collaborator.

Manage access

Add people

Select all — Type

Find a collaborator...

NSL Infotech Pvt LTD
GauravSethi-NSL · Collaborator

Previous Next

Whuups / **Whuups-code-2025-Mai-NSL-**

Type / to search

Code Issues Pull requests Actions Projects Security Insights Settings

Commits

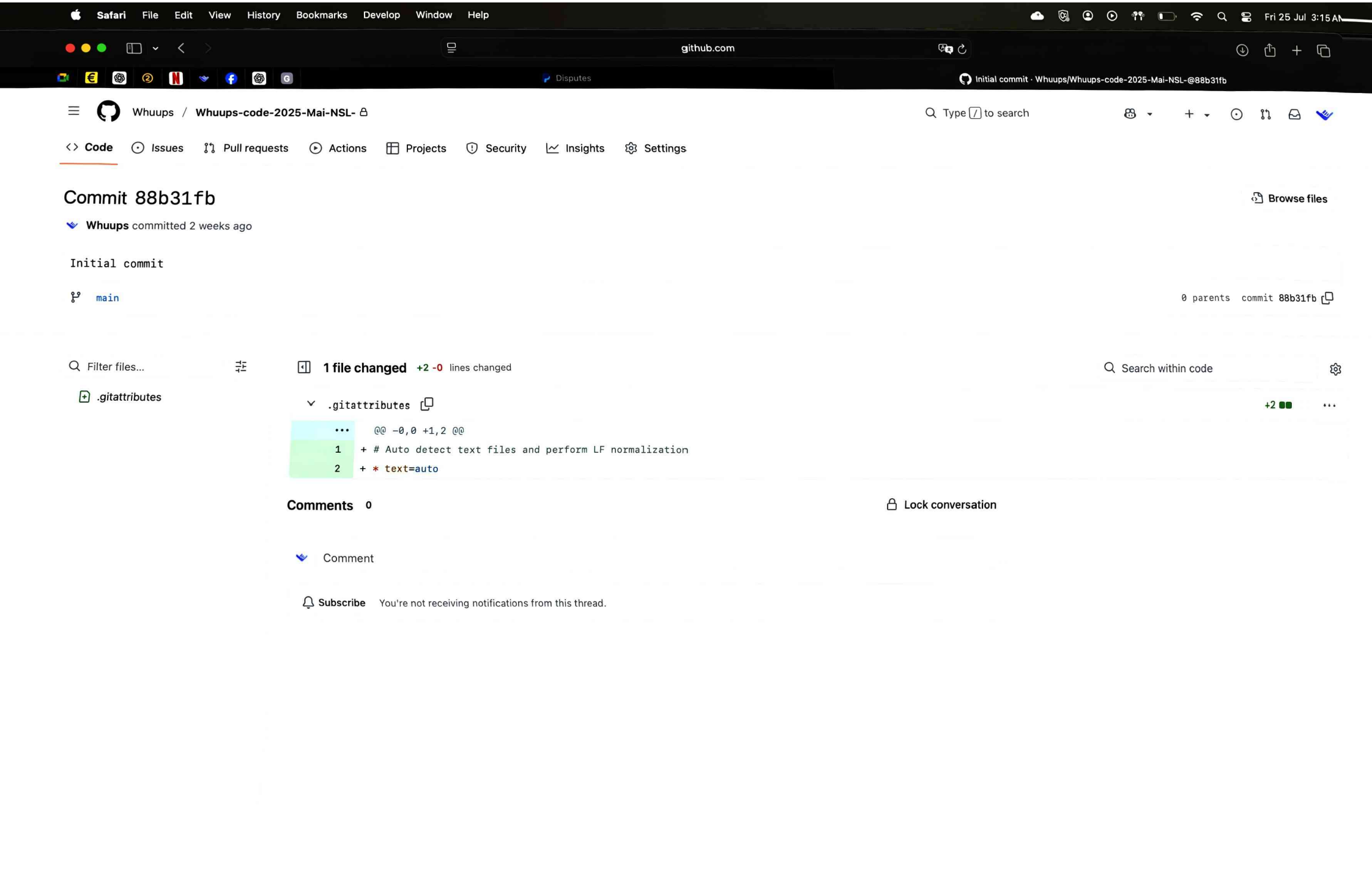
main

Whuups All time

Commits on Jul 8, 2025

Initial commit 88b31fb

Whuups committed 2 weeks ago


Safari File Edit View History Bookmarks Develop Window Help
Fri 25 Jul 3:15 AM
github.com
Disputes
Initial commit · Whuups/Whuups-code-2025-Mai-NSL-@88b31fb
Whuups / Whuups-code-2025-Mai-NSL-
Type / to search
Code Issues Pull requests Actions Projects Security Insights Settings
Commit 88b31fb
Browse files
Whuups committed 2 weeks ago
Initial commit
main
0 parents commit 88b31fb
Filter files...
.gitattributes
1 file changed +2 -0 lines changed
Search within code
.gitattributes
+2
@@ -0,0 +1,2 @@
+ # Auto detect text files and perform LF normalization
+ * text=auto
Comments 0
Lock conversation
Comment
Subscribe You're not receiving notifications from this thread.

Whuups / mobile2024

Type / to search

Code Issues Pull requests Actions Projects Security Insights Settings

Activity

All branches · All activity · All users · All time · Showing most recent first

Update README.md
Whuups pushed 1 commit to main · b48c1ef...3b2cda7 · on 18 Feb

Update README.md
Whuups pushed 1 commit to whuups_0.1 · 368b50e...4d0ff25 · on 18 Feb

adding the latest code
GauravSethi-NSL created whuups_0.1 · 368b50e · on 13 Feb

Deleted branch
GauravSethi-NSL deleted ios · on 8 Jan

Migrating code to github
GauravSethi-NSL created ios · 7d2a04a · on 20 Dec 2024

Update README.md
GauravSethi-NSL pushed 1 commit to master · 1d6b7ef...6426ce5 · on 28 Nov 2024

push to live
GauravSethi-NSL created master · 1d6b7ef · on 28 Nov 2024

Initial commit
Whuups created main · b48c1ef · on 23 Aug 2024

Share feedback about this page

domain=whuups.com&ident=s5svbgcn0ny3wshp

Sans action de votre part avant le 2024-11-01, le transfert sera effectué.

---------- ENGLISH VERSION
Attention: gbovrisse.mac@me.com
Re: Transfer of whuups.com

OVH received notification on 2024-10-27 that you have requested a transfer to another domain name registrar (PDR Ltd. d/b/a PublicDomainRegistry.com (IANA ID 303)).

If you want to PROCEED with this transfer, you do not need to respond to this message.

If you wish to CANCEL the transfer, please contact us before 2024-11-01 or please go
to our website :
https://www.ovh.com/fr/cgi-bin/domain/outgoing.cgi?domain=whuups.com&ident=s5svbgcn0ny3wshp

If we do not hear from you by 2024-11-01, the transfer will proceed.

L'équipe OVHcloud

Pour obtenir de l'aide, retrouvez toutes nos solutions en ligne sur notre Centre d'aide : https://help.ovhcloud.com/
Vous y retrouverez nos Guides, FAQ, Forum communautaire et Opérations de maintenance.