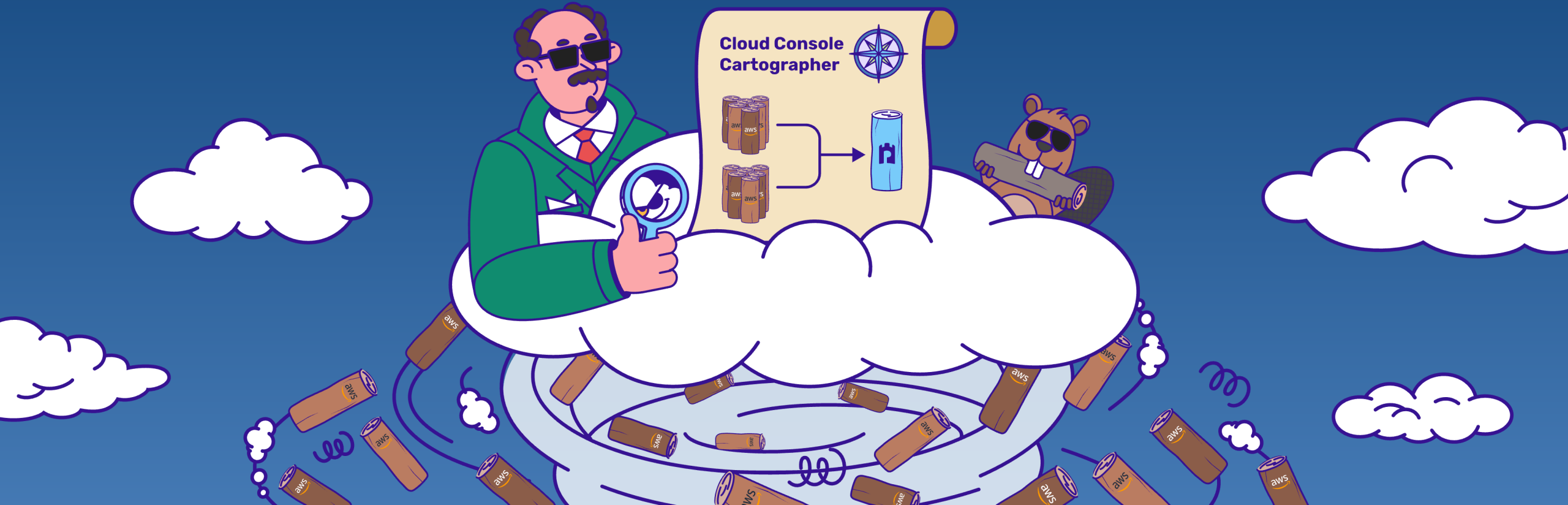



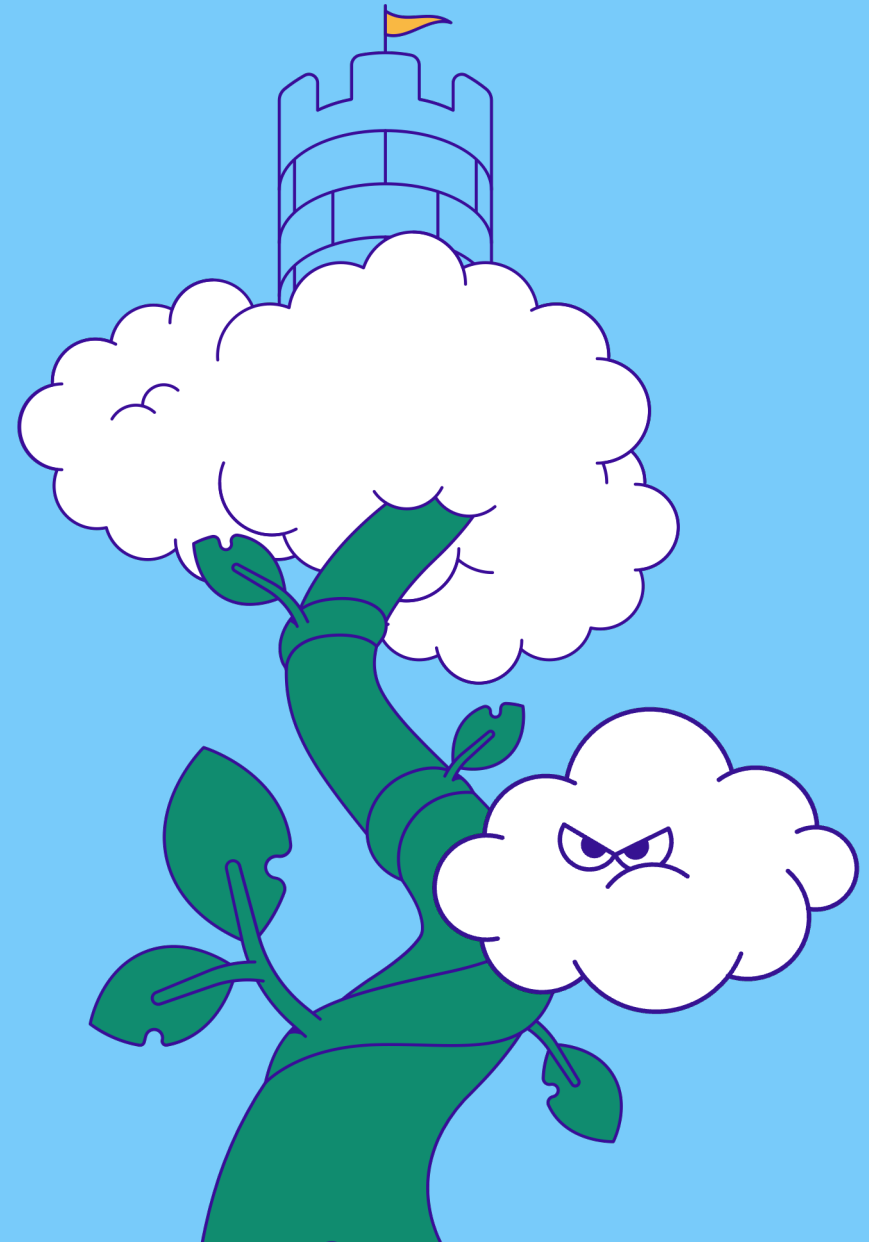
Cloud Console Cartographer

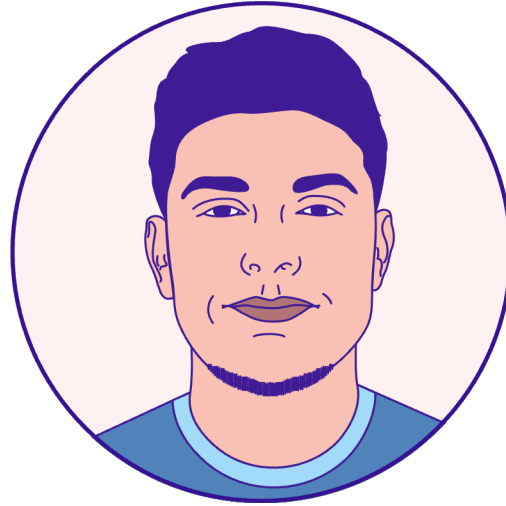
Tapping Into Mapping > Slogging Thru Logging



AGENDA

- Introduction 
- Cloud Logs for Defenders
- **PROBLEM:** Noisy Console Logs
- **SOLUTION:** Mapping for Clarity
- Tool Demo + Release





ANDI AHMETI

ASSOCIATE THREAT RESEARCHER



Kosovo



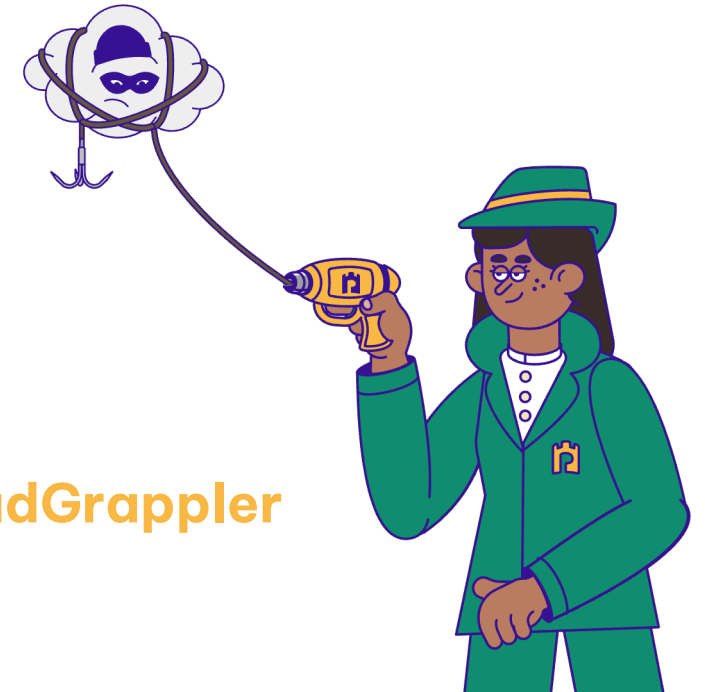
@SecEagleAnd1



andi-ahmeti



Permiso-io-tools/**CloudGrappler**





DANIEL BOHANNON

PRINCIPAL THREAT RESEARCHER



USA

MANDIANT (5 yrs)

 Microsoft (2 yrs)



@daniel**h**bohannon



daniel**h**bohannon

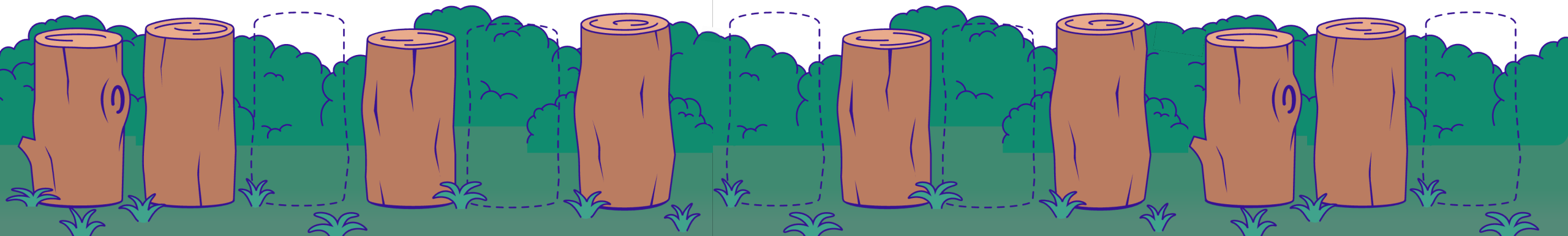
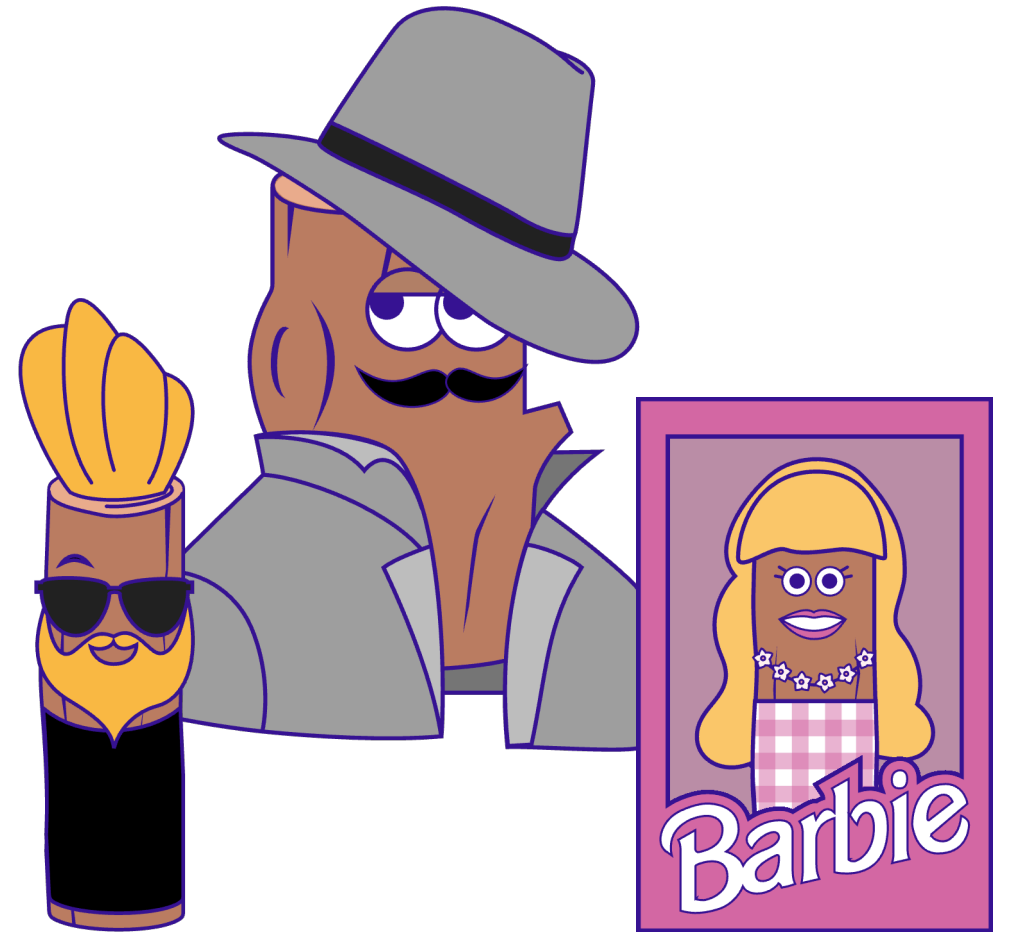


danielbohannon/**Invoke-Obfuscation**
/Invoke-CradleCrafter
/Invoke-DOSfuscation
/Revoke-Obfuscation



Role of Logs in Threat Hunting & IR

- Logs == Visibility
- Enable (if not by default)
- Forward to secondary location
- Process further:
 - Aggregate
 - Correlate
 - Search for malicious activity



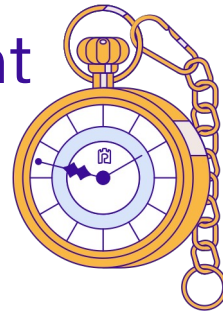
On-Prem vs Cloud Logs (*Data source, not storage location*)

- Host & network logs
- Native logging vs aftermarket products
- Extremely granular:
 - E.g. process arguments, image loads, process memory, registry modifications, DNS lookups, network connections, logon types, file writes, **file content**
- Numerous “**fingerprint**s” in user/attacker activity

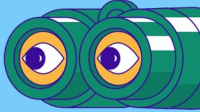


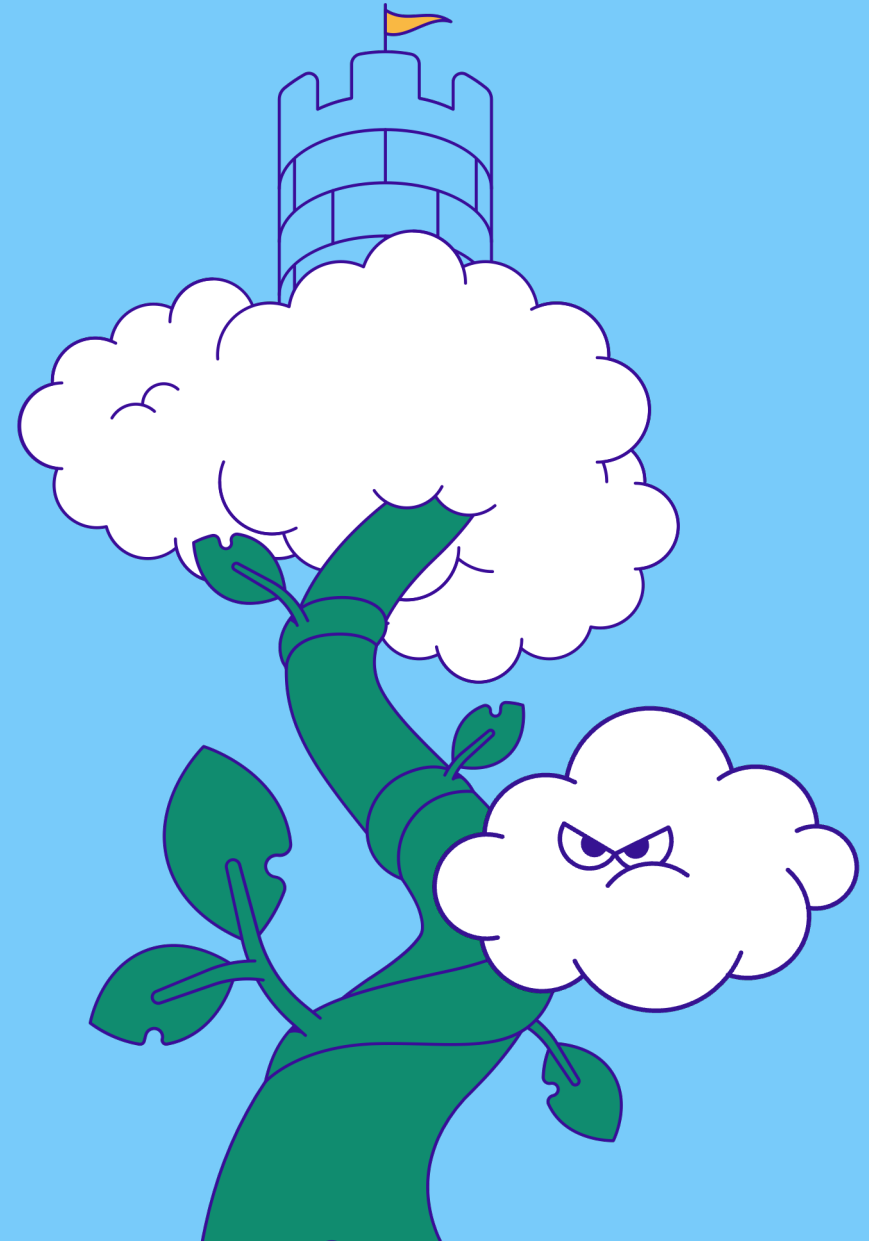
On-Prem vs Cloud Logs (*Data source, not storage location*)

- Determined by cloud provider
 - Control plane – management
 - Data plane – usage
- Delay in log generation
- Retention limits (if not forwarded)
- Far less granular / more abstracted
- Fewer “fingerprints” in user/attacker activity




AGENDA

- Introduction
- Cloud Logs for Defenders 
- PROBLEM: Noisy Console Logs
- SOLUTION: Mapping for Clarity
- Tool Demo + Release



Cloud Log Examples – Creating a User

```
{
  "eventTime": "2024-04-01T13:33:37.0000000Z",
  "userIdentity": { ... },
  "eventSource": "iam.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "userName": "krileva"
  },
  "responseElements": {
    "user": {
      "arn": "arn:aws:iam::200802171337:user/krileva",
      "userName": "krileva",
      "path": "/",
      "userId": "AIDA12345678ABCDEFGHI",
      "createDate": "Apr 1, 2024 1:33:37 PM"
    }
  },
  "readOnly": false,
  "eventType": "AwsApiCall",
  "sessionCredentialFromConsole": "true"
}
```

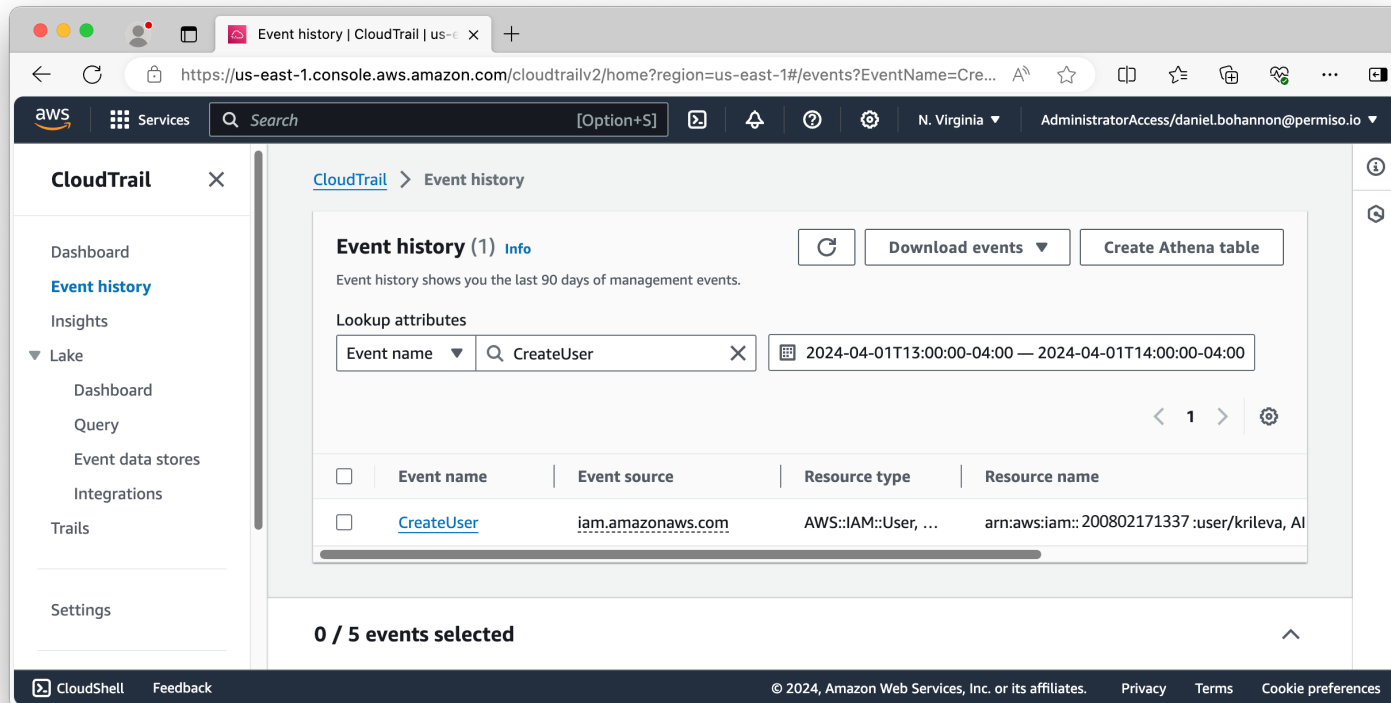


```
{
  "category": "UserManagement",
  "result": "success",
  "activityDisplayName": "Add user",
  "activityDateTime": "2024-04-01T13:33:37.1234567Z",
  "loggedByService": "Core Directory",
  "operationType": "Add",
  "initiatedBy": {},
  "targetResources": [
    {
      "id": "db014773-feed-acdc-beef-133337c0ffee",
      "displayName": null,
      "type": "User",
      "userPrincipalName": "krileva@permiso.io",
      "groupType": null,
      "modifiedProperties": [ { ... } ]
    }
  ],
  "additionalDetails": [],
  "eventType": "Add user",
  "createdDateTime": "2024-04-01T13:33:37.1234567Z",
  "fullName": "Core_Directory:UserManagement:Add_user"
}
```



Cloud Log Querying – API vs Forwarded

- API
 - PRO: Least delayed
 - CON: Limited retention (AWS = 90 days, Azure = 30 days)



The screenshot shows the AWS CloudTrail console interface. The main content area displays the 'Event history' for the 'CreateUser' event. The event details are as follows:

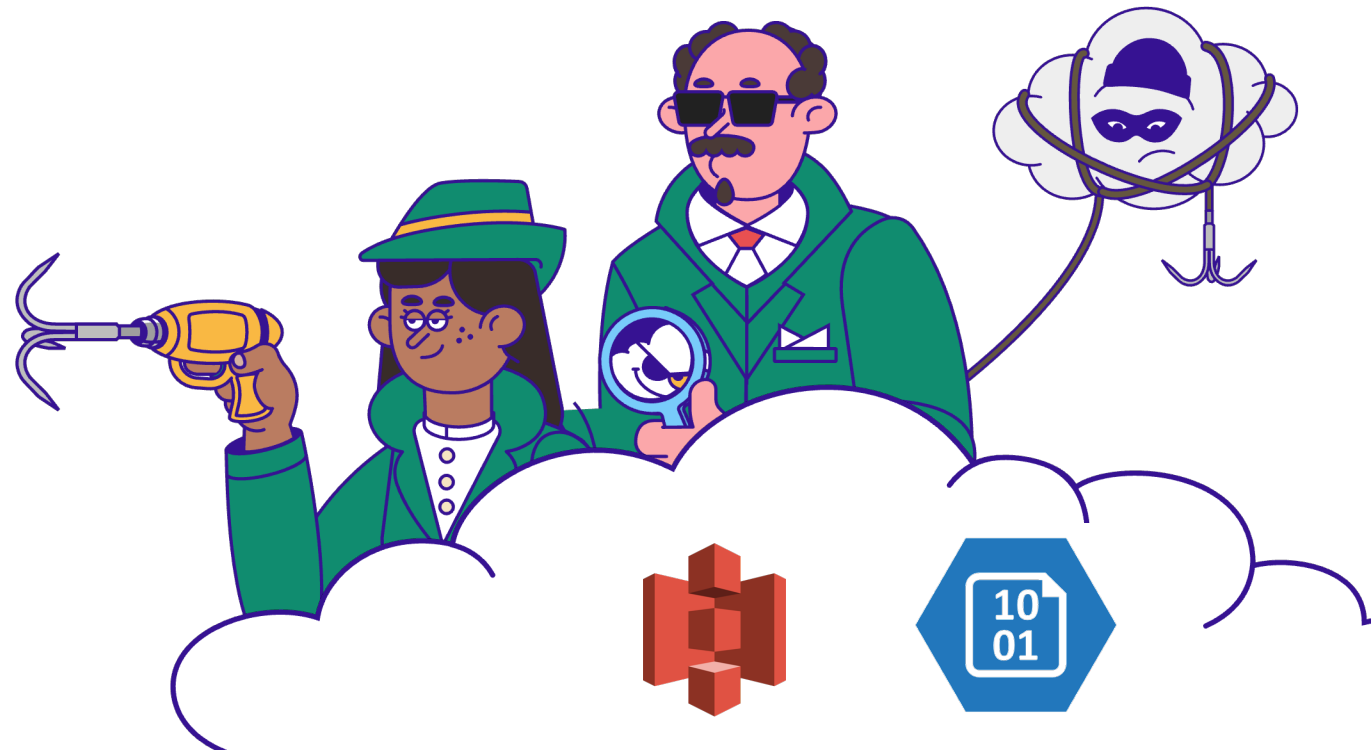
Event name	Event source	Resource type	Resource name
CreateUser	iam.amazonaws.com	AWS::IAM::User, ...	arn:aws:iam::200802171337:user/krileva, AI

At the bottom of the console, it indicates '0 / 5 events selected'.

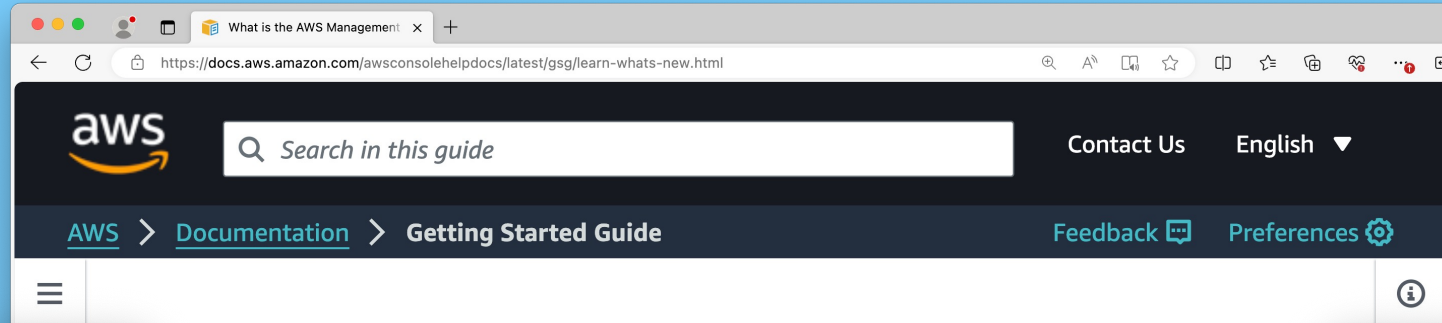
```
bash-3.2$
bash-3.2$ aws cloudtrail lookup-events \
> --lookup-attributes AttributeKey=EventName,AttributeValue=CreateUser \
> --start-time 2024-04-01T013:00:00 --end-time 2024-04-01T14:00:00
{
  "Events": [
    {
      "EventId": "db014773-abcd-1234-5678-133337c0ffee",
      "EventName": "CreateUser",
      "ReadOnly": "false",
      "AccessKeyId": "ASIA12345678ABCDEFGH",
      "EventTime": "2024-04-01T13:33:37-04:00",
      "EventSource": "iam.amazonaws.com",
      "Username": "andi.ahmeti@permiso.io",
      "Resources": [
        {
          "ResourceType": "AWS::IAM::User",
          "ResourceName": "arn:aws:iam::200802171337:user/krileva"
        },
        {
          "ResourceType": "AWS::IAM::User",
          "ResourceName": "AIDA12345678ABCDEFGHI"
        },
        {
          "ResourceType": "AWS::IAM::User",
          "ResourceName": "krileva"
        }
      ]
    },
    {
      "CloudTrailEvent": {
        "eventVersion": "1.09",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "AIDA12345678ABCDEFGHI",
          "arn": "arn:aws:iam::200802171337:user/andi.ahmeti@permiso.io",
          "accountId": "200802171337",
          "accessKeyId": "ASIA12345678ABCDEFGH",
          "userName": "andi.ahmeti@permiso.io",
          "sessionContext": {
            "attributes": {
              "creationDate": "2024-04-01T13:33:37Z",
              "mfaAuthenticated": "false"
            }
          },
          "eventTime": "2024-04-01T13:33:37Z",
          "eventSource": "iam.amazonaws.com",
          "eventName": "CreateUser",
          "awsRegion": "us-east-1",
          "sourceIPAddress": "13.33.33.37",
          "userAgent": "AWS Internal",
          "requestParameters": {
            "userName": "krileva"
          },
          "responseElements": {
            "user": {
              "path": "/",
              "userName": "krileva",
              "userId": "AIDA12345678ABCDEFGHI",
              "arn": "arn:aws:iam::200802171337:user/krileva",
              "createDate": "Apr 1, 2024 1:33:37 PM"
            }
          },
          "requestID": "db014773-feed-acdc-beef-133337c0ffee",
          "eventID": "db014773-abcd-1234-5678-133337c0ffee",
          "readOnly": "false",
          "eventType": "AwsApiCall",
          "managementEvent": "true",
          "recipientAccountId": "200802171337",
          "eventCategory": "Management",
          "sessionCredentialFromConsole": "true"
        }
      }
    }
  ]
}
```


Cloud Log Querying – API vs Forwarded

- API
 - PRO: Least delayed
 - CON: Limited retention (AWS = 90 days, Azure = 30 days)
- Forwarded
 - PRO: Unlimited storage
 - PRO: No API throttling
 - PRO: Easier consumption by other tools
 - CON: Missing event metadata
 - CON: Add'l monitoring



Definition: Console



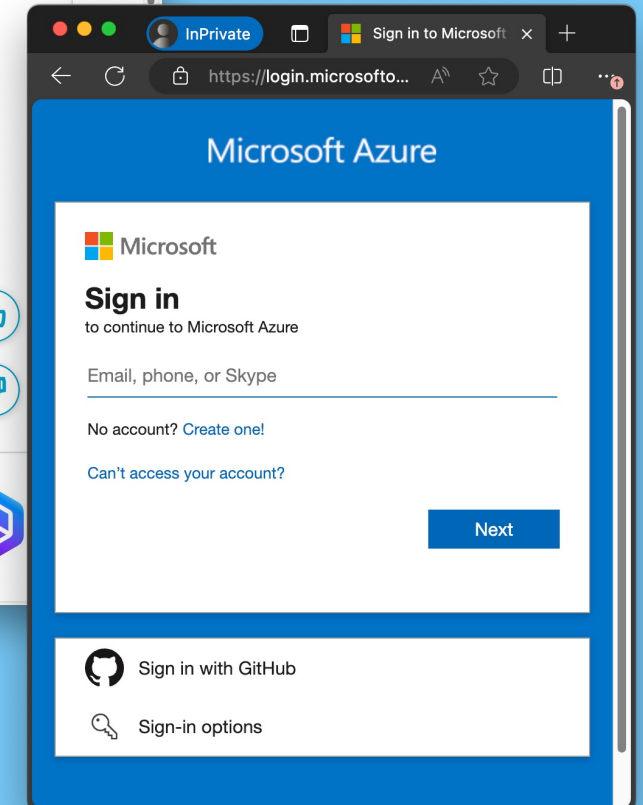
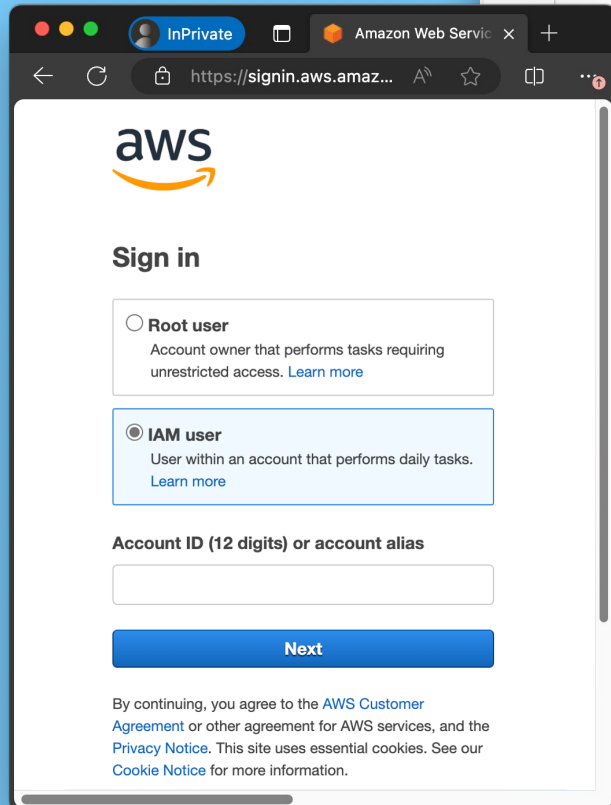
What is the AWS Management Console?

PDF

The [AWS Management Console](#) is a web application that comprises and refers to a broad collection of service consoles for managing AWS resources.

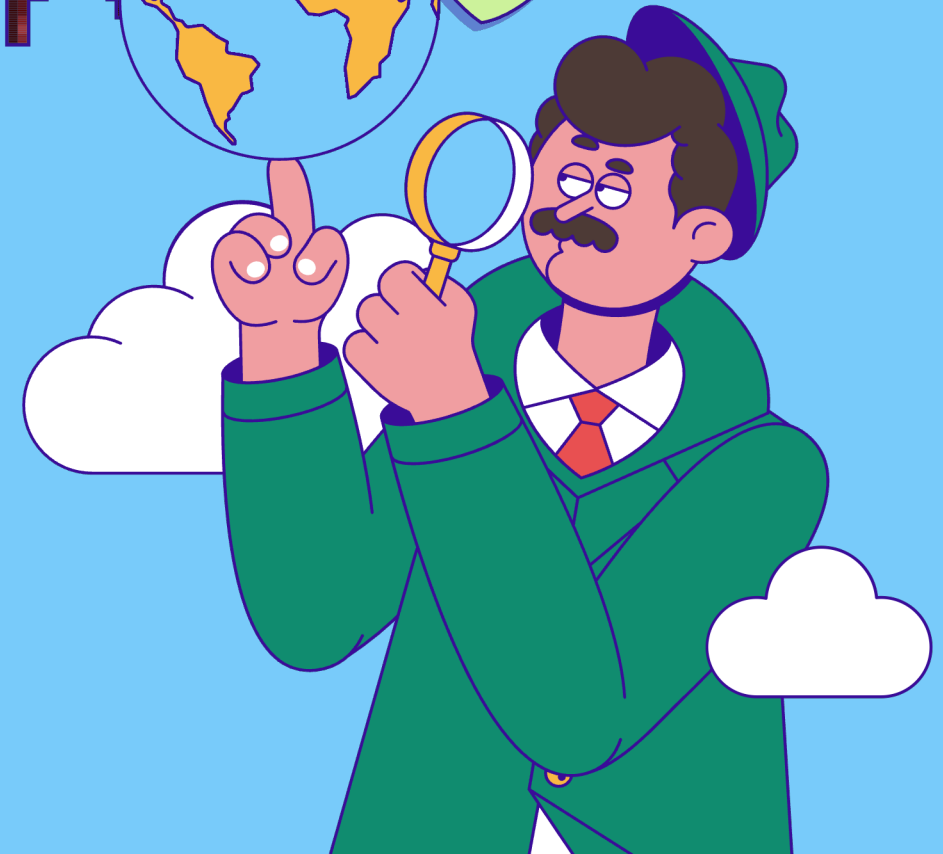
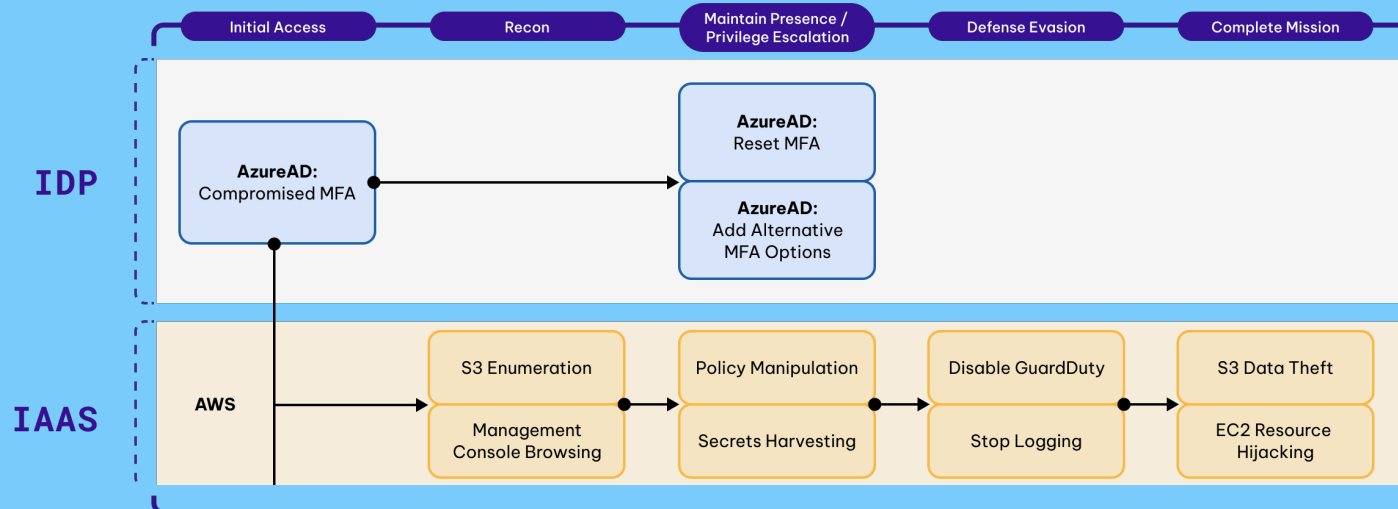
When you first sign in, you see the console home page. The home page provides access to each service console and offers a single place to access the information you need to perform your AWS related tasks. It also lets

```
{  
  "eventSource": "signin.amazonaws.com",  
  "eventName": "ConsoleLogin",  
  "eventType": "AwsConsoleSignIn"  
}
```



Console Usage in the Wild

- Threat actors
 - LUCR-1
 - aka GUI-vil
 - LUCR-3
 - aka Scattered Spider, Roasted Oktopus, UNC3944, STORM-0875 (Octo Tempest)



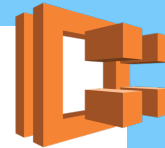
Console Usage in the Wild

- Threat actors
 - LUCR-1
 - aka GUI-vil
 - LUCR-3
 - aka Scattered Spider, Roasted Octopus, UNC3944, STORM-0875 (Octo Tempest)



Permissions

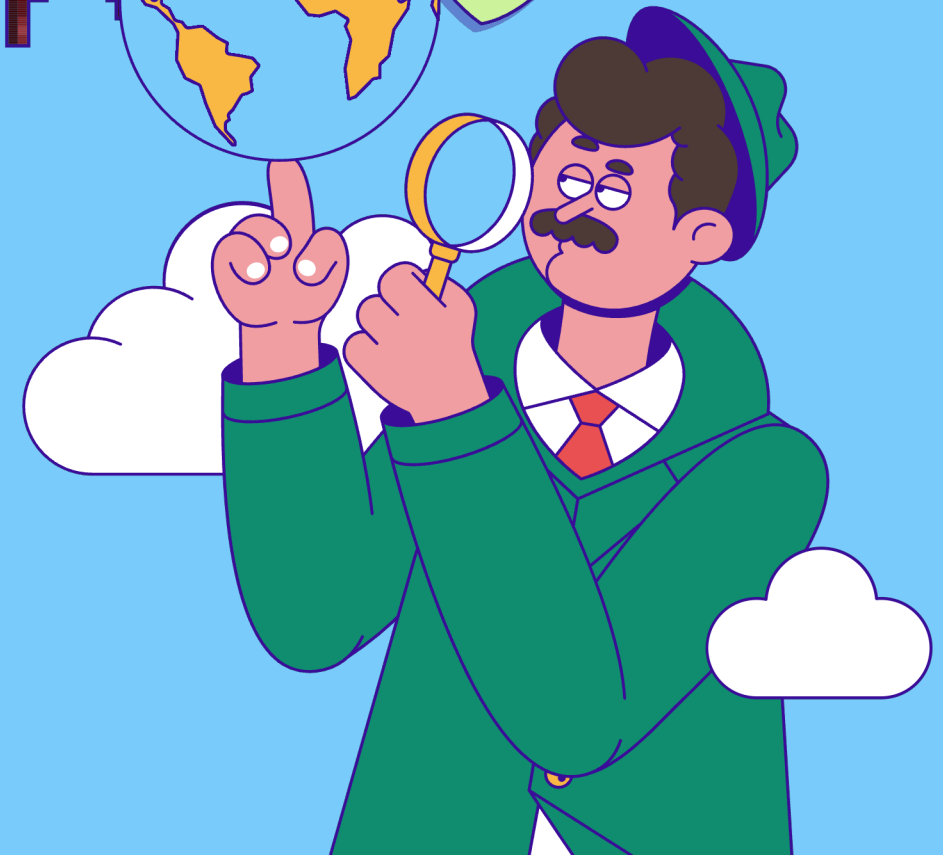
`sts:GetFederationToken`

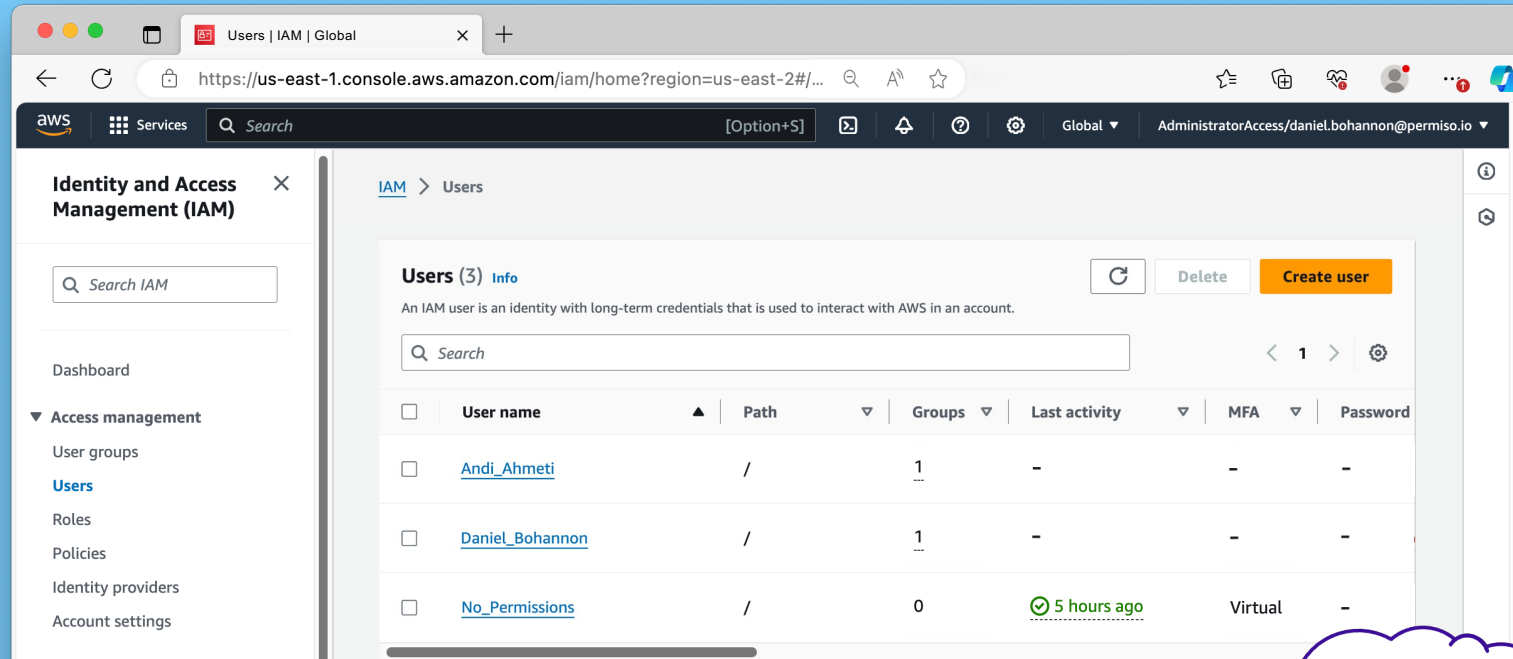


You can use the temporary credentials created by `GetFederationToken` in any AWS service with the following exceptions:

- You cannot call any IAM operations using the AWS CLI or the AWS API. This limitation does not apply to console sessions.
- You cannot call any AWS STS operations except `GetCallerIdentity`.

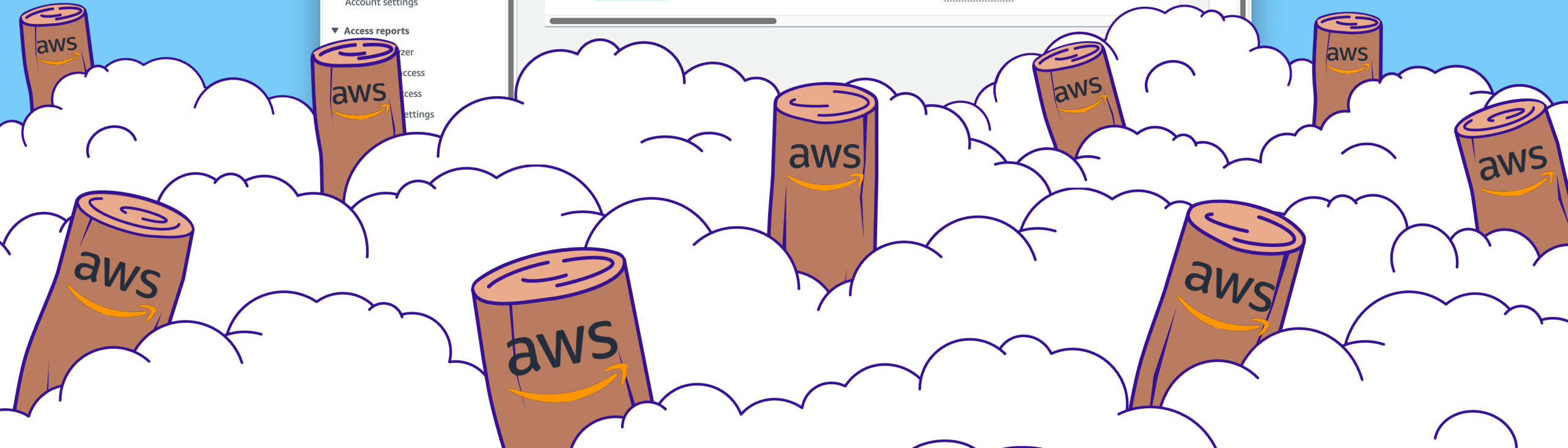
You can use temporary credentials for single sign-on (SSO) to the console.

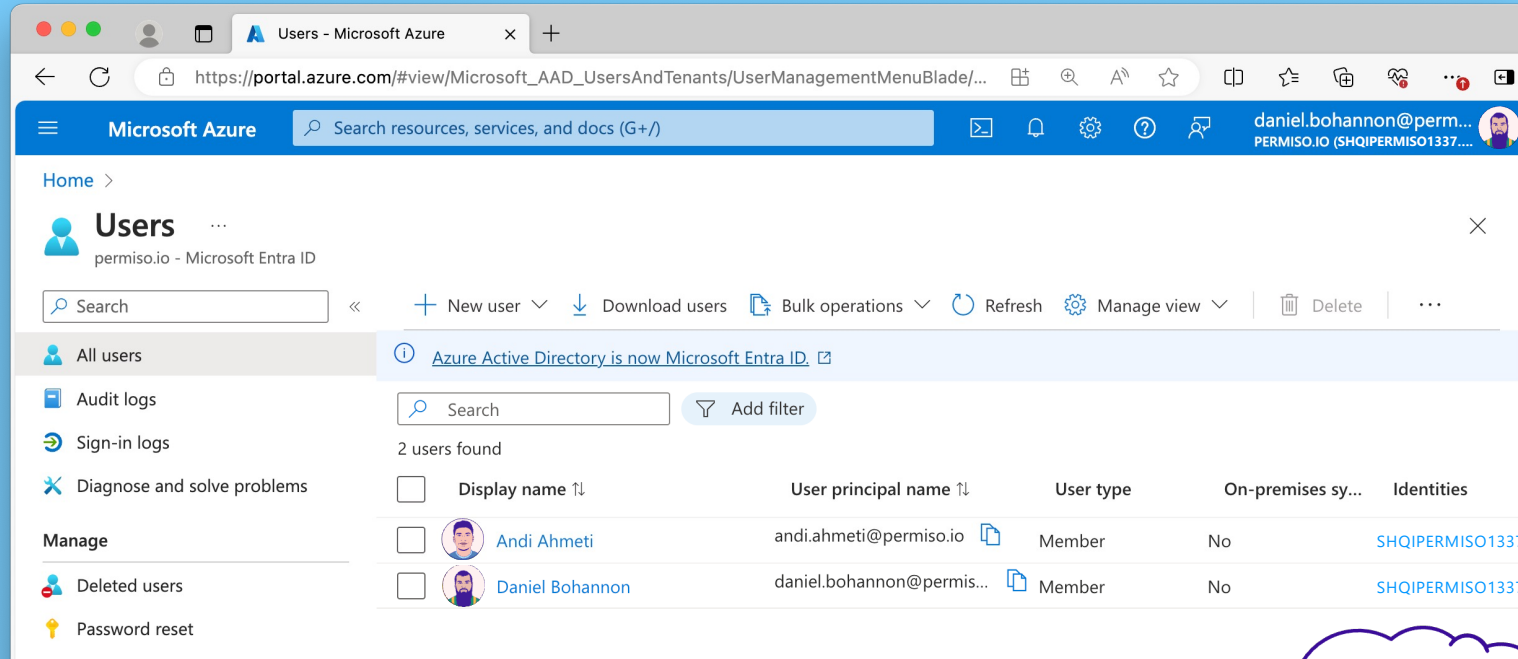




The screenshot shows the AWS IAM console interface. The browser address bar displays the URL: `https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#...`. The page title is "Users | IAM | Global". The left sidebar contains the "Identity and Access Management (IAM)" menu with options like "Search IAM", "Dashboard", "Access management", "Access reports", "User groups", "Roles", "Policies", "Identity providers", "Account settings", "User", "Access", "Access", and "Settings". The main content area is titled "IAM > Users" and shows "Users (3) Info". Below this, there is a search bar and a table of users. The table has columns for "User name", "Path", "Groups", "Last activity", "MFA", and "Password".

<input type="checkbox"/>	User name	Path	Groups	Last activity	MFA	Password
<input type="checkbox"/>	Andi_Ahmeti	/	1	-	-	-
<input type="checkbox"/>	Daniel_Bohannon	/	1	-	-	-
<input type="checkbox"/>	No_Permissions	/	0	5 hours ago	Virtual	-





Microsoft Azure

Search resources, services, and docs (G+)

daniel.bohannon@perm...
PERMISO.IO (SHQIPERMISO1337...)

Users

permiso.io - Microsoft Entra ID

Search

+ New user | Download users | Bulk operations | Refresh | Manage view | Delete

All users [Azure Active Directory is now Microsoft Entra ID](#)



Audit logs

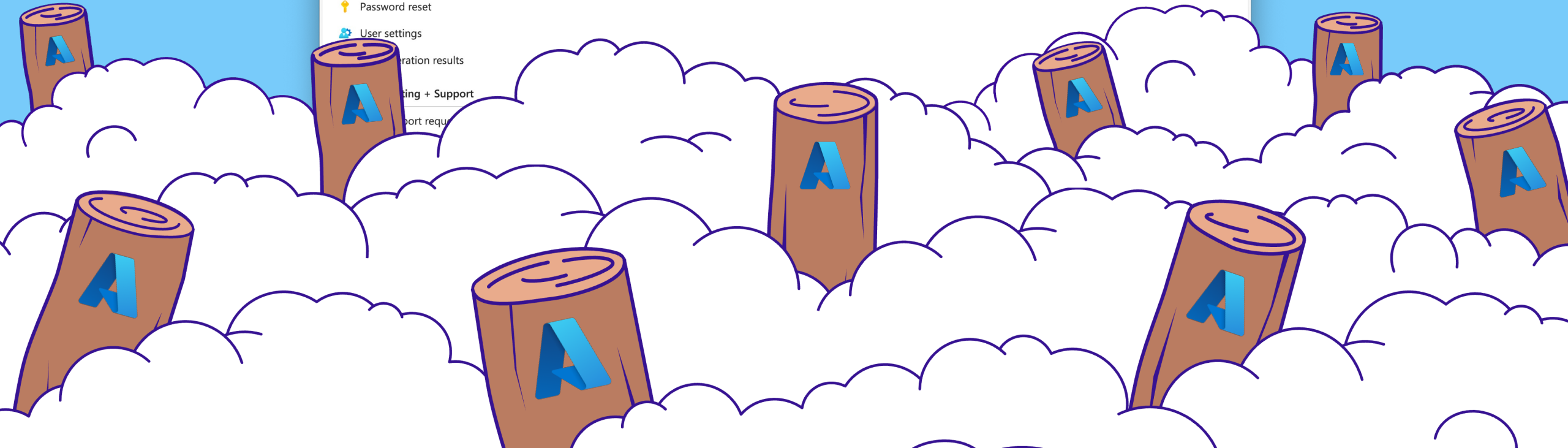
Sign-in logs

Diagnose and solve problems

Manage

- Deleted users
- Password reset
- User settings
- Registration results
- Getting + Support
- Support request

<input type="checkbox"/>	Display name ↓	User principal name ↓	User type	On-premises sy...	Identities
<input type="checkbox"/>	 Andi Ahmeti	andi.ahmeti@permiso.io	Member	No	SHQIPERMISO1337...
<input type="checkbox"/>	 Daniel Bohannon	daniel.bohannon@permis...	Member	No	SHQIPERMISO1337...





Users - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/...

Microsoft Azure Search resources, services, and docs (G+)

daniel.bohannon@perm... PERMISO.IO (SHQIPERMISO1337...)

Home >

Users

permiso.io - Microsoft Entra ID

Search

+ New user | Download users | Bulk operations | Refresh | Manage view | Delete

All users [Azure Active Directory is now Microsoft Entra ID](#)

Audit logs Search Add filter

Sign-in logs

Diagnose and solve problems

Manage

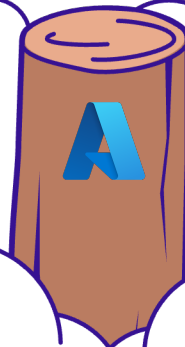
- Deleted users
- Password reset
- User settings
- Bulk operation results

Troubleshooting + Support

New support request

2 users found

<input type="checkbox"/>	Display name ↓	User principal name ↓	User type	On-premises sy...	Identities
<input type="checkbox"/>	Andi Ahmeti	andi.ahmeti@permiso.io	Member	No	SHQIPERMISO1337...
<input type="checkbox"/>	Daniel Bohannon	daniel.bohannon@permis...	Member	No	SHQIPERMISO1337...





Users - Microsoft Azure

https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/...

Microsoft Azure Search resources, services, and docs (G+)

daniel.bohannon@perm... PERMISO.IO (SHQIPERMISO1337...)

Home >

Users

permiso.io - Microsoft Entra ID

Search

+ New user | Download users | Bulk operations | Refresh | Manage view | Delete

All users [Azure Active Directory is now Microsoft Entra ID](#)

Audit logs Search Add filter

Sign-in logs

Diagnose and solve problems

Manage

Deleted users

Password reset

User settings

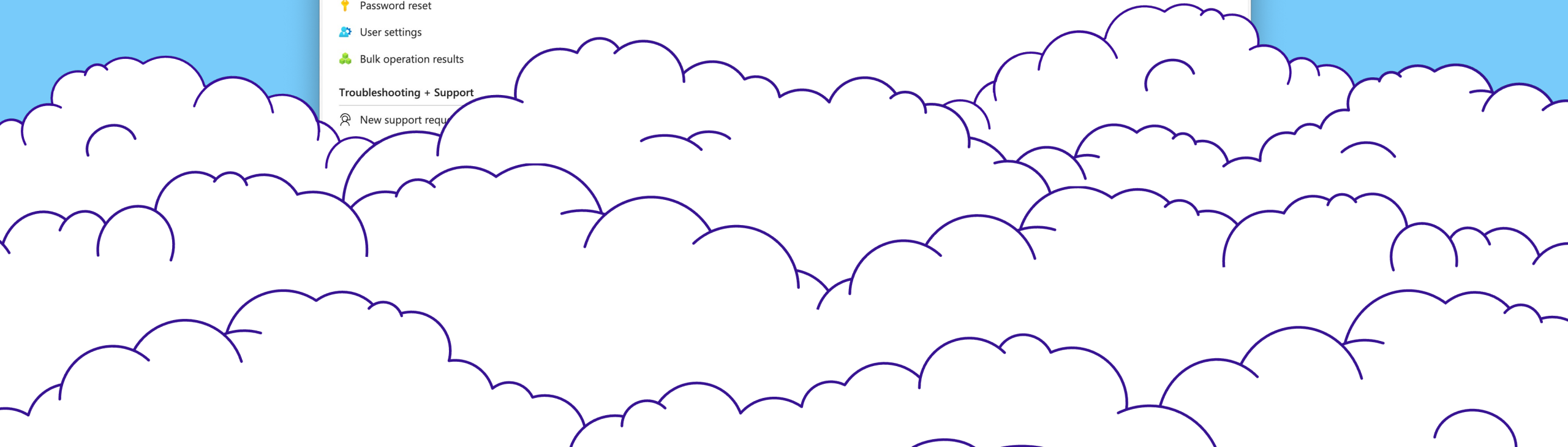
Bulk operation results

Troubleshooting + Support

New support request

2 users found

<input type="checkbox"/>	Display name ↓	User principal name ↓	User type	On-premises sy...	Identities
<input type="checkbox"/>	Andi Ahmeti	andi.ahmeti@permiso.io	Member	No	SHQIPERMISO1337...
<input type="checkbox"/>	Daniel Bohannon	daniel.bohannon@permis...	Member	No	SHQIPERMISO1337





NO, N-NOT YOU,

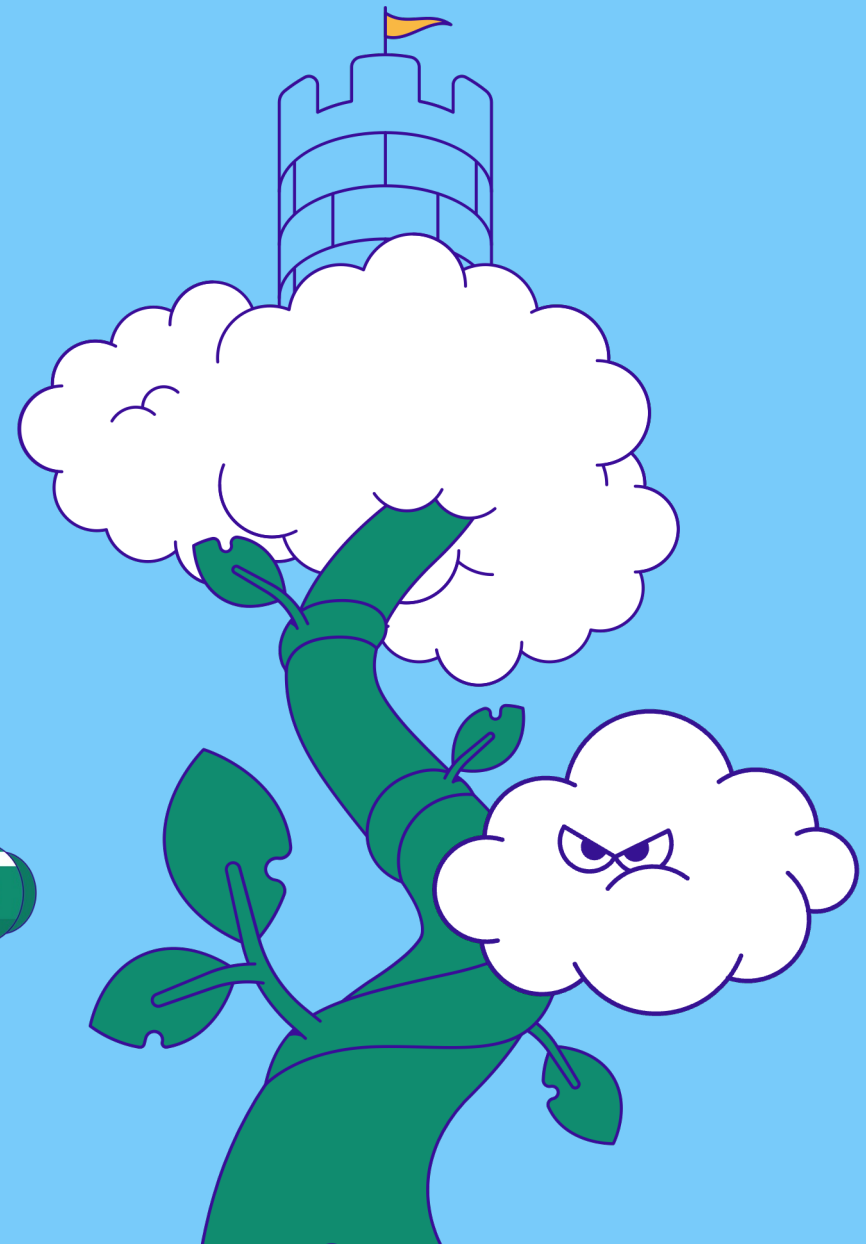
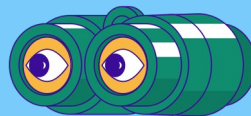


aws



AGENDA

- Introduction
- Cloud Logs for Defenders
- **PROBLEM:** Noisy Console Logs
- **SOLUTION:** Mapping for Clarity
- Tool Demo + Release



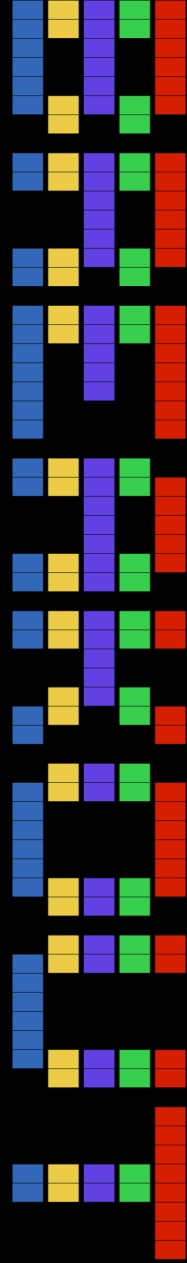
AGENDA

- **PROBLEM: Noisy Console Logs** 👁 👁



ATARI

PERMISO



No Permissions – 1/3 – Console Home

The screenshot shows the AWS Console Home page for a user with no permissions. The page is titled "Console Home" and includes a search bar and a user profile "No_Permissions @ 2008-0217-1337". The main content area is divided into several sections:

- Recently visited:** Shows a single entry for "IAM".
- Applications (0):** Shows a "Create application" button and a search bar. Below the search bar, there is an "Access denied" error message: "You don't have permission to `servicecatalog:ListApplications`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)"
- Welcome to AWS:** Includes a link to "Getting started with AWS" and "Training and certification".
- AWS Health:** Shows "No health data" and a message: "You don't have permissions to".
- Cost and usage:** Shows an "Access denied" error message: "You don't have permission to `ce:GetCostAndUsage`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)" Below the error, the following details are listed:
 - User: User:
 - Service: ce
 - Action: GetCostAndUsage

The footer of the page includes "CloudShell", "Feedback", "© 2024, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

No Permissions – 1/3 – Console Home



servicecatalog:ListApplications

ce:GetCostAndUsage

The screenshot shows the AWS Console Home page with an 'Access denied' error message. The error message is displayed in a red box and reads: "You don't have permission to request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)" Below the error message, the following text is displayed: "User: User", "Service: ce", and "Action: GetCostAndUsage".

No Permissions – 1/3 – Console Home



The screenshot shows the AWS IAM console home page. The search bar contains 'IAM' and the search results are displayed in a list. The results are categorized into Services and Features. The Services list includes IAM, IAM Identity Center, Resource Access Manager, and AWS App Mesh. The Features list includes Groups, Roles, and Policies. A 'No health data' message is displayed at the bottom of the search results, indicating that the user does not have permissions to view the health data. A 'No_Permissions' error message is visible in the top right corner of the console.

Search results for 'IAM'

Services (11) See all 11 results ▶

- IAM** Manage access to AWS resources
- IAM Identity Center** Manage workforce user access to multiple AWS accounts and cloud applications
- Resource Access Manager** Share AWS resources with other accounts or AWS Organizations
- AWS App Mesh** Easily monitor and control microservices

Features (22) See all 22 results ▶

- Groups** IAM feature
- Roles** IAM feature
- Policies** IAM feature

No health data
You don't have permissions to

copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: User:
Service: ce
Action: GetCostAndUsage

servicecatalog:ListApplications

ce:GetCostAndUsage

No Permissions – 2/3 – IAM Dashboard



servicecatalog>ListApplications

ce:GetCostAndUsage

The screenshot shows the AWS IAM Dashboard with three 'Access denied' error messages:

- Access denied**
You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
Action: GetAccountSummary
On resource(s): *
- Access denied**
You don't have permission to `iam:ListMFADevices`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
Action: ListMFADevices
On resource(s): user
- Access denied**
You don't have permission to `iam:ListAccessKeys`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

Other visible elements include the 'AWS Account' section with an error for `iam:ListAccountAliases` and the 'Quick Links' section with a link to 'My security credentials'.

No Permissions – 2/3 – IAM Dashboard



The screenshot shows the AWS IAM Dashboard with three 'Access denied' error messages:

- Access denied**: You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
Action: GetAccountSummary
On resource(s): *
- Access denied**: You don't have permission to `iam:ListMFADevices`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
Action: ListMFADevices
On resource(s): user
- Access denied**: You don't have permission to `iam:ListAccessKeys`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

servicecatalog:ListApplications

ce:GetCostAndUsage

iam:ListAccountAliases

iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

No Permissions – 2/3 – IAM Dashboard



The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with sections for 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Related consoles'. The main content area displays two 'Access denied' error messages. The first error message states: 'You don't have permission to [action] on resource(s) [resource]. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.' Below this, the details are: 'User: arn:aws:iam::200802171337:user/No_Permissions', 'Service: iam', 'Action: ListMFADevices', and 'On resource(s): user'. A 'Copy' button is present. The second error message follows a similar format but for the action 'GetAccountSummary' and resource '*'. The right sidebar contains 'Quick Links' (My security credentials), 'Tools' (Policy simulator), and 'Additional information' (Security best practices in IAM, IAM documentation).

servicelog:ListApplications

ce:GetCostAndUsage

iam:ListAccountAliases

iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

No Permissions – 2/3 – IAM Dashboard



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options like 'Dashboard', 'Access management', 'Access reports', and 'Related consoles'. The main content area displays two 'Access denied' messages. The first message is for the action 'ListMFADevices' on resource 'user'. The second message is for the action 'GetAccountSummary' on resource '*'. Both messages include a 'Copy' button and a link to 'Learn more about troubleshooting access denied errors'.

servicelog:ListApplications

ce:GetCostAndUsage

iam:ListAccountAliases

iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

iam:GetAccountSummary

No Permissions – 3/3 – IAM Users



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options under 'Identity and Access Management (IAM)', with 'Users' highlighted by a yellow arrow. The main content area displays 'Users (0)' with a 'Create user' button. Below this, a table header is visible with columns for 'User name', 'Path', 'Groups', 'Last activity', 'MFA', and 'Password'. A large red error box is overlaid on the table, containing the following text:

Access denied
You don't have permission to `iam:ListUsers`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
Action: ListUsers
On resource(s): arn:aws:iam::200802171337:user/
Context: no identity-based policy allows the iam:ListUsers action

A 'Copy' button is located next to the error details.

servicecatalog:ListApplications

ce:GetCostAndUsage

iam:ListAccountAliases

iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

iam:GetAccountSummary

No Permissions – 3/3 – IAM Users



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options under 'Identity and Access Management (IAM)', with 'Users' highlighted by a yellow arrow. The main content area displays the 'Users (0)' page, which is currently empty. A large red error box is overlaid on the page, indicating an 'Access denied' error. The error message states: 'You don't have permission to [redacted]. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)' Below the message, a text box contains the following details: 'User: arn:aws:iam::200802171337:user/No_Permissions', 'Service: iam', 'Action: ListUsers', 'On resource(s): arn:aws:iam::200802171337:user/', and 'Context: no identity-based policy allows the iam:ListUsers action'. A 'Copy' button is located to the right of the text box.

servicecatalog:ListApplications

ce:GetCostAndUsage

iam:ListAccountAliases

iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

iam:GetAccountSummary

iam:ListUsers

No Permissions - 3/3 - IAM Users



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options: Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, Credential report, Organization activity, Service control policies (SCPs)), and Related consoles (IAM Identity Center, AWS Organizations). The main content area is titled 'Users (0) Info' and shows an 'Access denied' message. The error details are as follows:

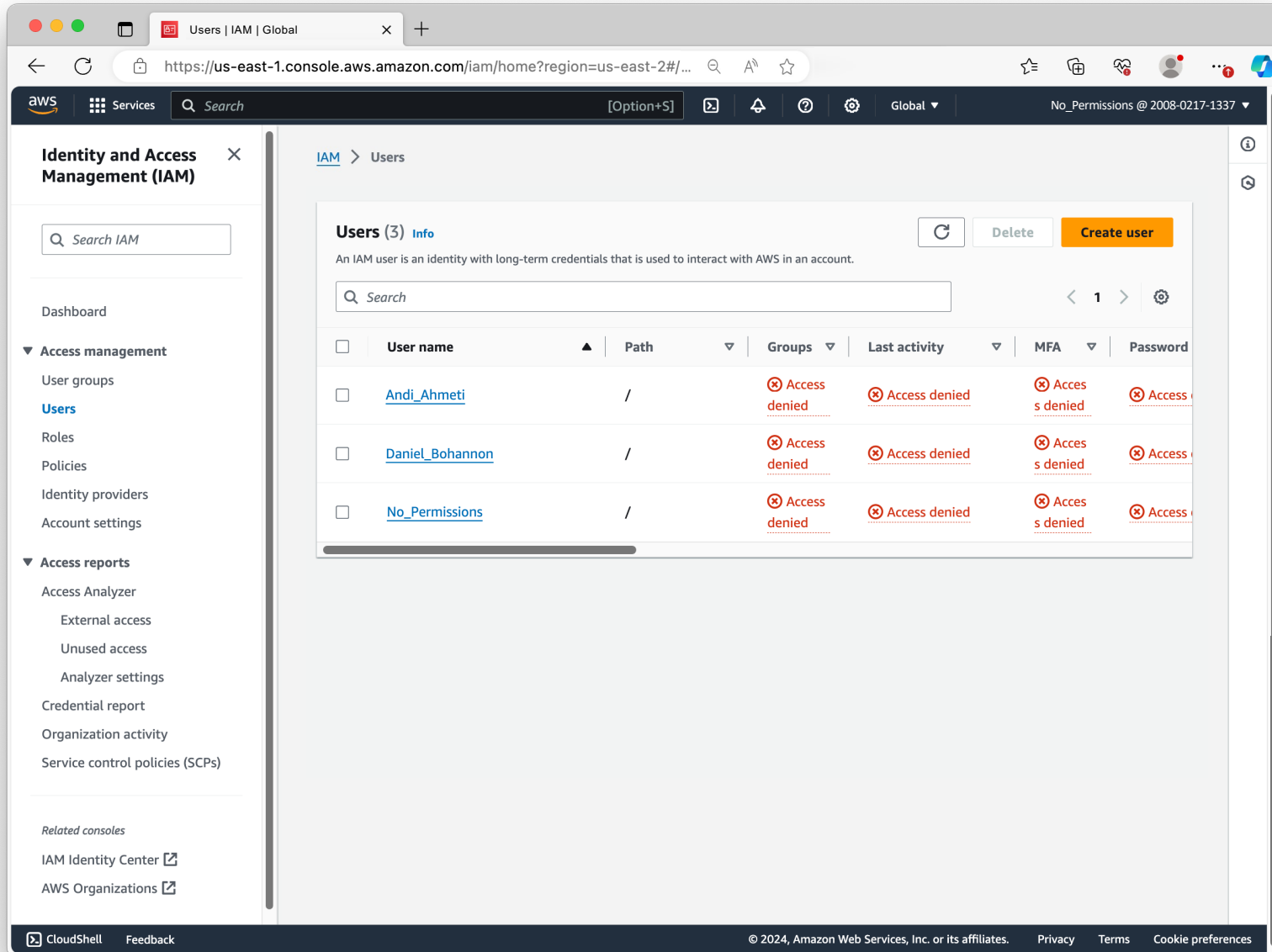
```
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
Action: ListUsers
On resource(s): arn:aws:iam::200802171337:user/
Context: no identity-based policy allows the iam:ListUsers action
```

The error message also includes a 'Copy' button and a link to 'Learn more about troubleshooting access denied errors.' The console footer shows '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

iam:ListUsers



No Permissions – 3/3 – IAM Users



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options for Identity and Access Management (IAM), including Access management, Access reports, and Related consoles. The main content area displays the 'Users (3) Info' section, which includes a search bar and a table of users. The table lists three users: Andi_Ahmeti, Daniel_Bohannon, and No_Permissions. Each user has a checkbox, a path, and columns for Groups, Last activity, MFA, and Password. All users have 'Access denied' status in the Groups, Last activity, and MFA columns. The No_Permissions user also has 'Access denied' in the Password column. A 'Create user' button is visible at the top right of the user list.

User name	Path	Groups	Last activity	MFA	Password
Andi_Ahmeti	/	Access denied	Access denied	Access denied	Access denied
Daniel_Bohannon	/	Access denied	Access denied	Access denied	Access denied
No_Permissions	/	Access denied	Access denied	Access denied	Access denied



```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "VisualEditor0",  
      "Effect": "Allow",  
      "Action": "iam:ListUsers",  
      "Resource": "*" }  
  ]  
}
```



No Permissions – 3/3 – IAM Users

The screenshot shows the AWS IAM console interface. The main content area displays the 'Users (3)' page with a table of users. An 'Access denied' modal is open, showing the error message: 'You don't have permission to iam:ListGroupForUser. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.' The modal also displays the following details:

- User: arn:aws:iam::200802171337:user/No_Permissions
- Service: iam
- Action: ListGroupsForUser
- On resource(s): Andi_Ahmeti

The table in the background shows columns for User name, Path, Groups, Last activity, MFA, and Password, with several 'Access denied' icons in the Last activity column.



```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "VisualEditor0",  
      "Effect": "Allow",  
      "Action": "iam:ListUsers",  
      "Resource": "*" }  
  ]  
}
```



Console Mapping – IAM Users

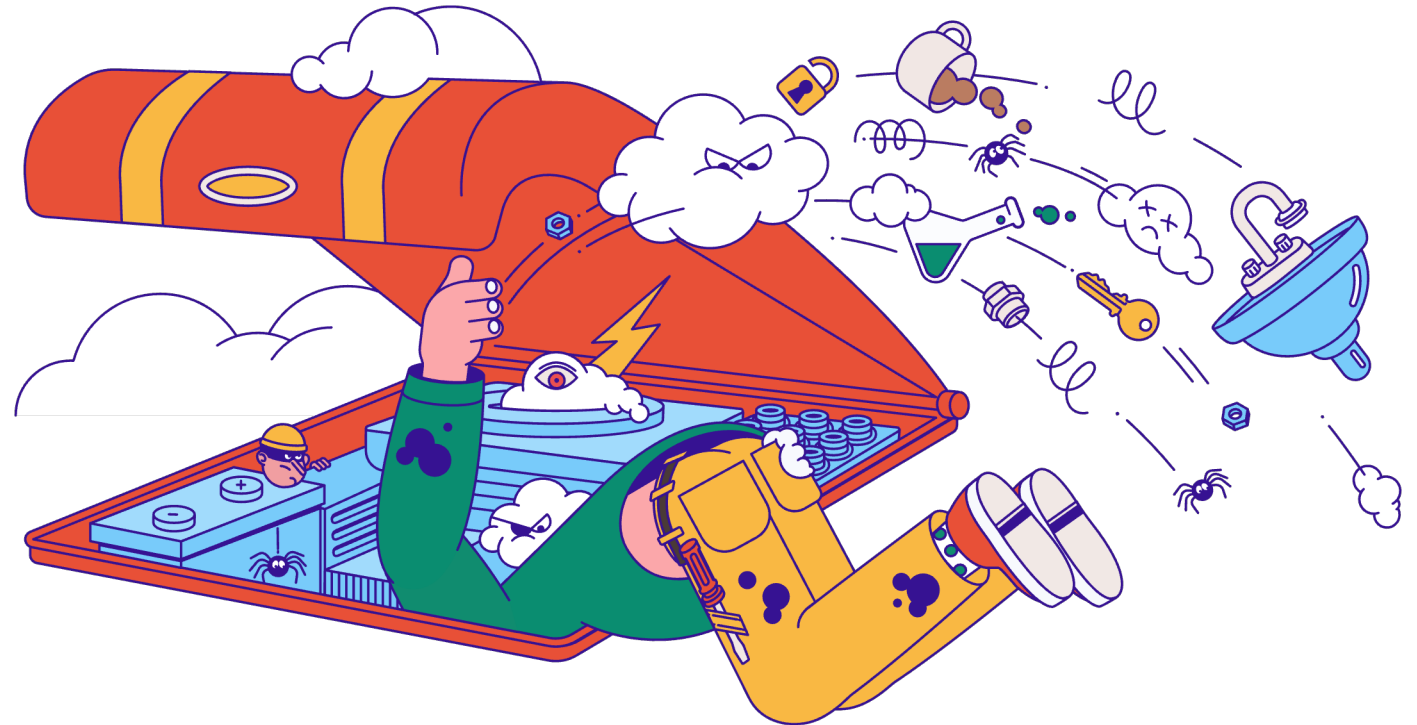


Console Mapping – IAM Users



“Open the Hood” of Console Logs

- Full Permissions
- New Environment (per service)
- Excel Spreadsheet
- Lots of Coffee



Console Mapping – IAM Users



A

Users (0) Info Info Refresh Delete Create user

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

< 1 > Settings

User name	Path	Groups	Last activity	MFA	Password
<div><p>Access denied</p><p>You don't have permission to <i>iam:ListUsers</i>. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.</p><pre>User: arn:aws:iam::200802171337:user/No_Permissions Service: iam Action: ListUsers On resource(s): arn:aws:iam::200802171337:user/ Context: no identity-based policy allows the iam:ListUsers action</pre>Copy</div>					

B

Users (3) Info Info Refresh Delete Create user

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

< 1 > Settings

User name	Path	Groups	Last activity	MFA	Password
<input type="checkbox"/> Andi_Ahmeti	/	Access denied	Access denied	Access denied	Access denied
<input type="checkbox"/> Daniel_Bohannon	/	Access denied	Access denied	Access denied	Access denied
<input type="checkbox"/> No_Permissions	/	Access denied	Access denied	Access denied	Access denied

C

Users (3) Info Info Refresh Delete Create user

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

< 1 > Settings

User name	Path	Groups	Last activity	MFA	Password
<input type="checkbox"/> Andi_Ahmeti	/	1	-	-	-
<input type="checkbox"/> Daniel_Bohannon	/	1	-	-	-
<input type="checkbox"/> No_Permissions	/	0	5 hours ago	Virtual	-

Console Mapping – IAM Users

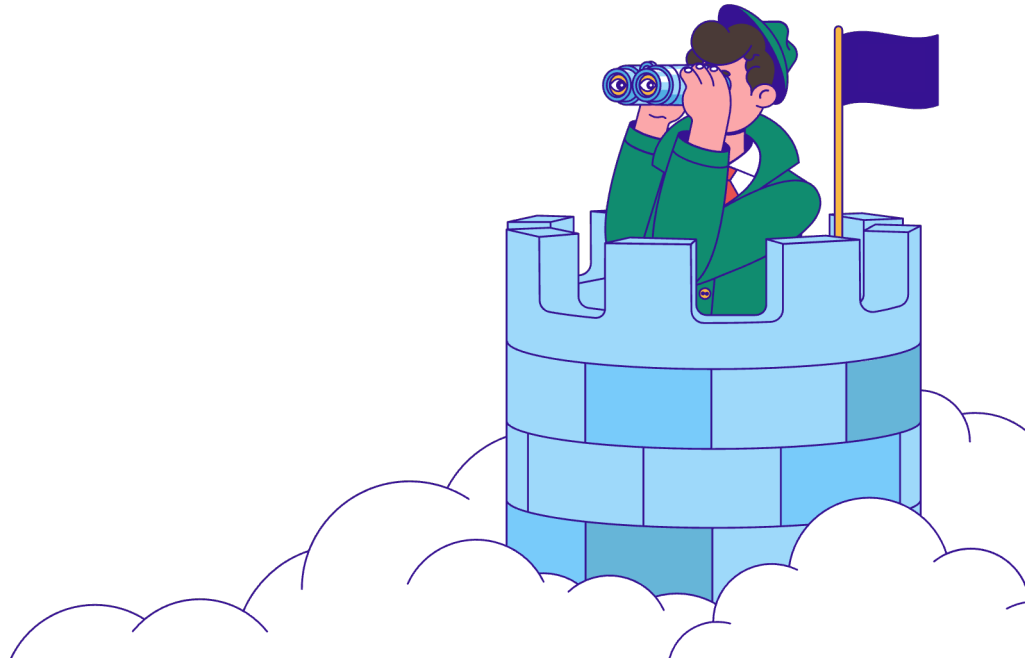


A

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:13:37.0000	iam:ListUsers	AWS Internal		AccessDenied

B

C



Console Mapping – IAM Users



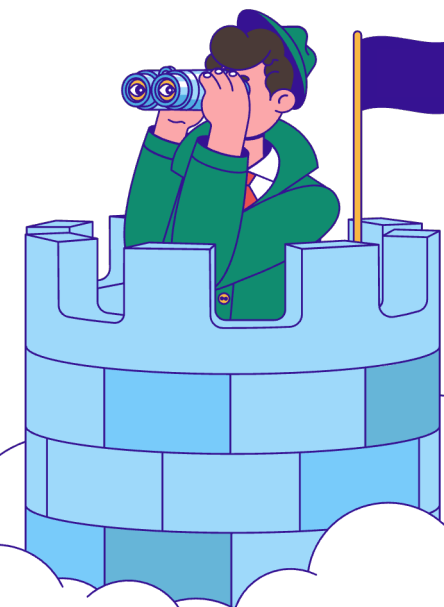
A

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:13:37.0000	iam:ListUsers	AWS Internal		AccessDenied

B

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:17:16.0000	iam:ListUsers	AWS Internal	{"maxItems":1000}	
2024-03-18 04:17:17.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...		AccessDenied

C



Console Mapping – IAM Users



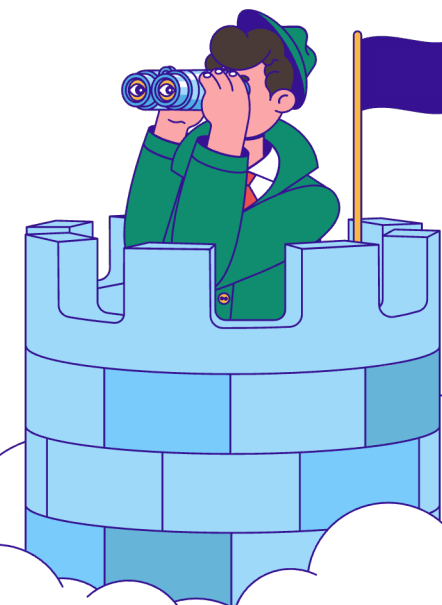
A

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:13:37.0000	iam:ListUsers	AWS Internal		AccessDenied

B

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:17:16.0000	iam:ListUsers	AWS Internal	{"maxItems":1000}	
2024-03-18 04:17:17.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...		AccessDenied

C



Console Mapping – IAM Users



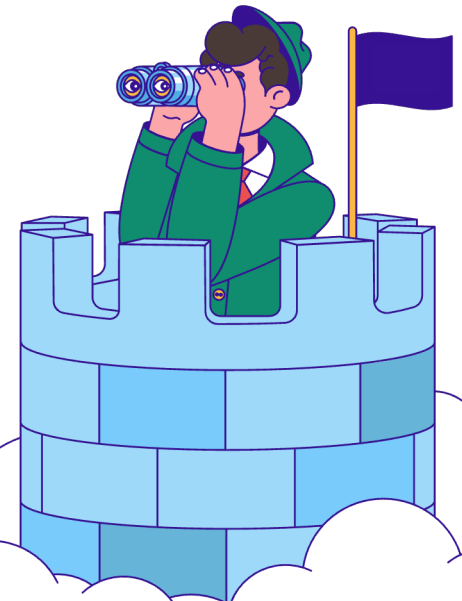
A

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:13:37.0000	iam:ListUsers	AWS Internal		AccessDenied

B

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:17:16.0000	iam:ListUsers	AWS Internal	{"maxItems":1000}	
2024-03-18 04:17:17.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000		aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:20.0000		aws-internal/3 aws-sdk-java/...		AccessDenied

C



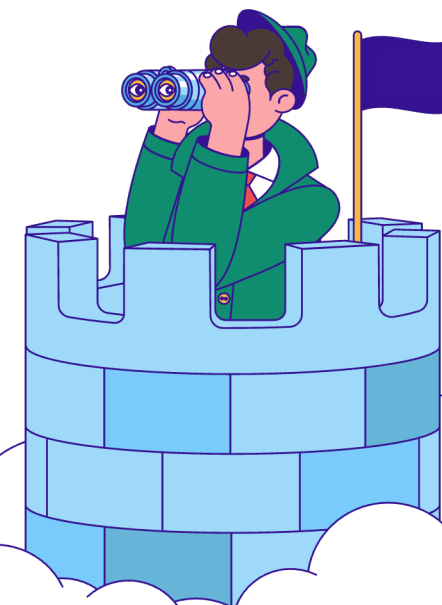
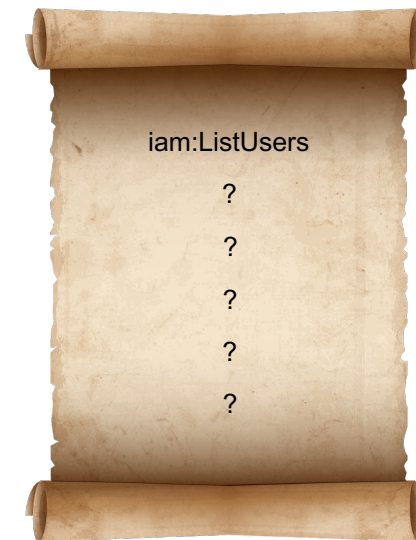
Console Mapping – IAM Users

A

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:13:37.0000	iam:ListUsers	AWS Internal		AccessDenied

C

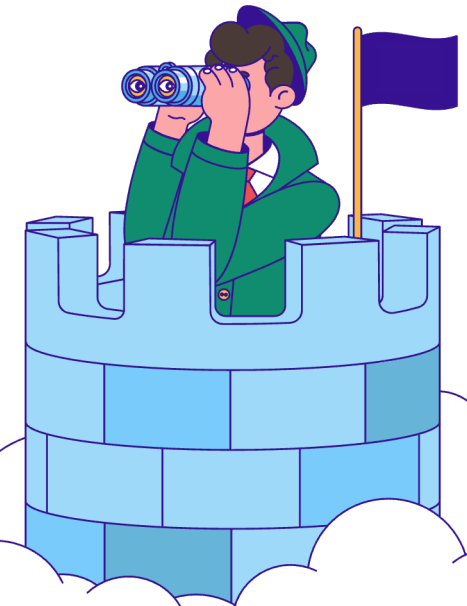
eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:20:50.0000	iam:ListUsers	AWS Internal	{"maxItems":1000}	
2024-03-18 04:20:51.0000		aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}	
2024-03-18 04:20:51.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}	
2024-03-18 04:20:51.0000		aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}	
2024-03-18 04:20:52.0000		aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}	
2024-03-18 04:20:52.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}	
2024-03-18 04:20:52.0000		aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}	
2024-03-18 04:20:53.0000		aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}	
2024-03-18 04:20:53.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}	
2024-03-18 04:20:53.0000		aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}	
2024-03-18 04:20:54.0000		aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}	
2024-03-18 04:20:54.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}	
2024-03-18 04:20:54.0000		aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}	
2024-03-18 04:20:54.0000		aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}	
2024-03-18 04:20:54.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}	
2024-03-18 04:20:54.0000		aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}	
2024-03-18 04:20:55.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}	
2024-03-18 04:20:55.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}	



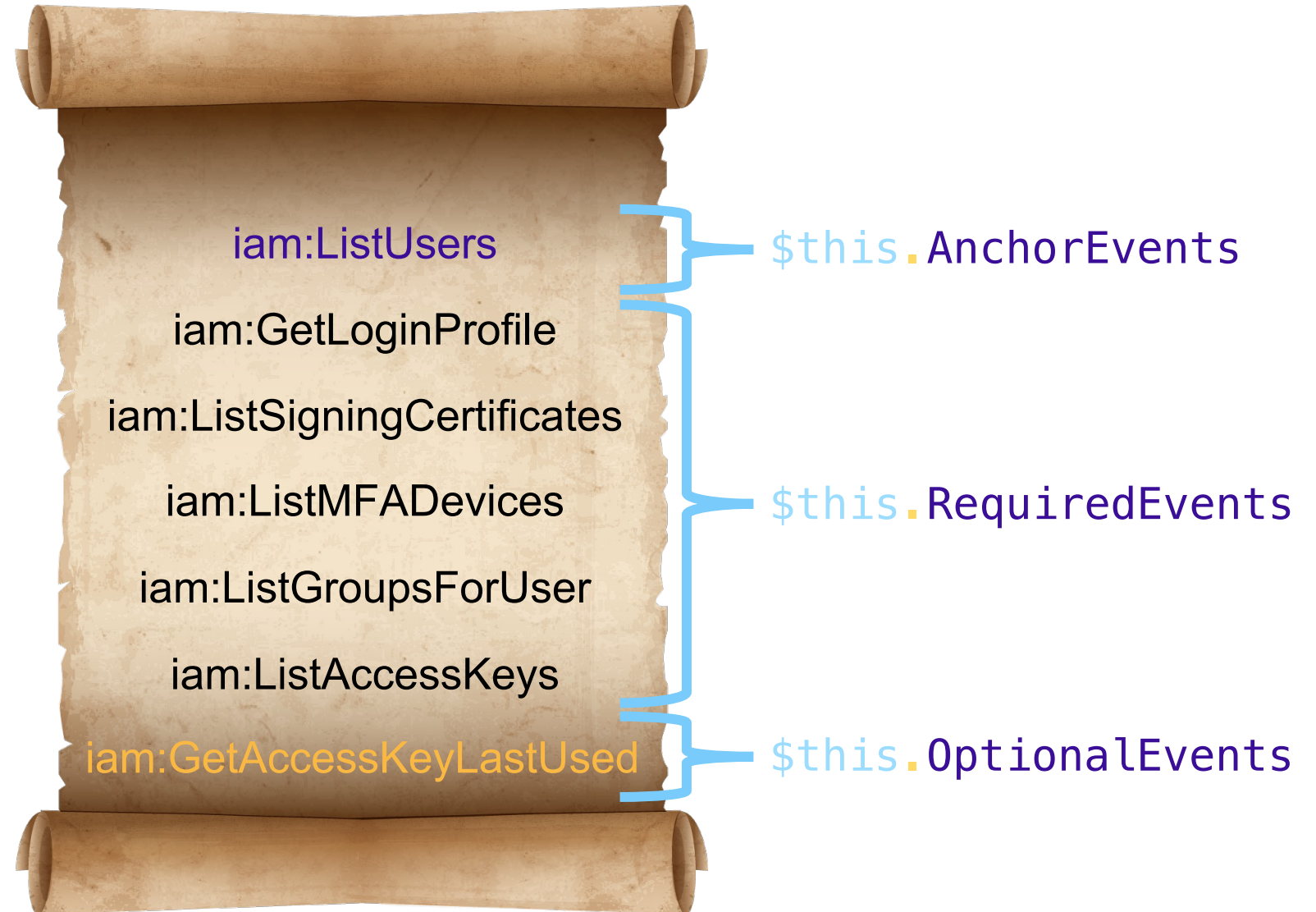
Console Mapping – IAM Users

Name	Access Key ID	Created	Last Used
iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...		{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...		{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}

iam:ListUsers
iam:GetLoginProfile
iam:ListSigningCertificates
iam:ListMFADevices
iam:ListGroupsForUser
iam:ListAccessKeys



Console Mapping – IAM Users



Console Mapping – OptionalEvents (Background)

eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:19:43.0000	ec2:DescribeRegions	Mozilla/5.0 (Macintosh; Intel ...	{"regionSet":{},"allRegions":true}
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"eventStatusCodes":["open","u
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"eventStatusCodes":["open"],
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"startTimes":{"from":"Mar 11
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"startTimes":{"from":"Mar 11
2024-03-18 04:19:43.0000	notifications:ListNotificationHubs	Mozilla/5.0 (Macintosh; Intel ...	
2024-03-18 04:19:44.0000	ce:GetCostAndUsage	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"Values":
2024-03-18 04:19:44.0000	ce:GetCostForecast	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"Values"
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"eventStatusCodes":["open","upcoming
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"eventStatusCodes":["open"],"startTim
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"eventStatusCodes":["open"],"startTi
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"startTimes":{"from":"Mar 11, 2024
2024-03-18 04:19:44.0000	servicecatalog-appregistry:ListApplications	Mozilla/5.0 (Macintosh; Intel ...	{"maxResults":"100"}



Console Mapping – OptionalEvents (Background)

ConsoleHome			
eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:19:43.0000	ec2:DescribeRegions	Mozilla/5.0 (Macintosh; Intel ...	{"regionSet":{},"allRegions":true}
2024-03-18 04:19:44.0000	ce:GetCostAndUsage	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"V
2024-03-18 04:19:44.0000	ce:GetCostForecast	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"
2024-03-18 04:19:44.0000	servicecatalog-appregistry:ListApplications	Mozilla/5.0 (Macintosh; Intel ...	{"maxResults":"100"}
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"startTimes":[{"from":"Mar 11
2024-03-18 04:19:43.0000	notifications:ListNotificationHubs	Mozilla/5.0 (Macintosh; Intel ...	
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"eventStatusCodes":["open","upcoming
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"eventStatusCodes":["open"],"startTim
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"eventStatusCodes":["open"],"startTi
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"startTimes":[{"from":"Mar 11, 2024



Console Mapping – OptionalEvents (Background)

ConsoleHome

eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:19:43.0000	ec2:DescribeRegions	Mozilla/5.0 (Macintosh; Intel ...	{"regionSet":{},"allRegions":true}
2024-03-18 04:19:44.0000	ce:GetCostAndUsage	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"V
2024-03-18 04:19:44.0000	ce:GetCostForecast	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"
2024-03-18 04:19:44.0000	servicecatalog-appregistry:ListApplications	Mozilla/5.0 (Macintosh; Intel ...	{"maxResults":"100"}

eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"eventStatusCodes":["open","upcoming
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"eventStatusCodes":["open"],"startTim
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"startTimes":[{"from":"Mar 11, 2024 4
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"startTimes":[{"from":"Mar 11, 2024,
2024-03-18 04:19:43.0000	notifications:ListNotificationHubs	Mozilla/5.0 (Macintosh; Intel ...	
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"eventStatusCodes":["open","upcom
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"eventStatusCodes":["open"],"startT
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"eventStatusCodes":["open"],"startT
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"startTimes":[{"from":"Mar 11, 2024 4



Console Mapping – OptionalEvents (Background)

ConsoleHome			
eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:19:43.0000	ec2:DescribeRegions	Mozilla/5.0 (Macintosh; Intel ...	{"regionSet":{},"allRegions":true}
2024-03-18 04:19:44.0000	ce:GetCostAndUsage	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"V
2024-03-18 04:19:44.0000	ce:GetCostForecast	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"
2024-03-18 04:19:44.0000	servicecatalog-appregistry:ListApplications	Mozilla/5.0 (Macintosh; Intel ...	{"maxResults":"100"}



Console Mapping – OptionalEvents (Context)

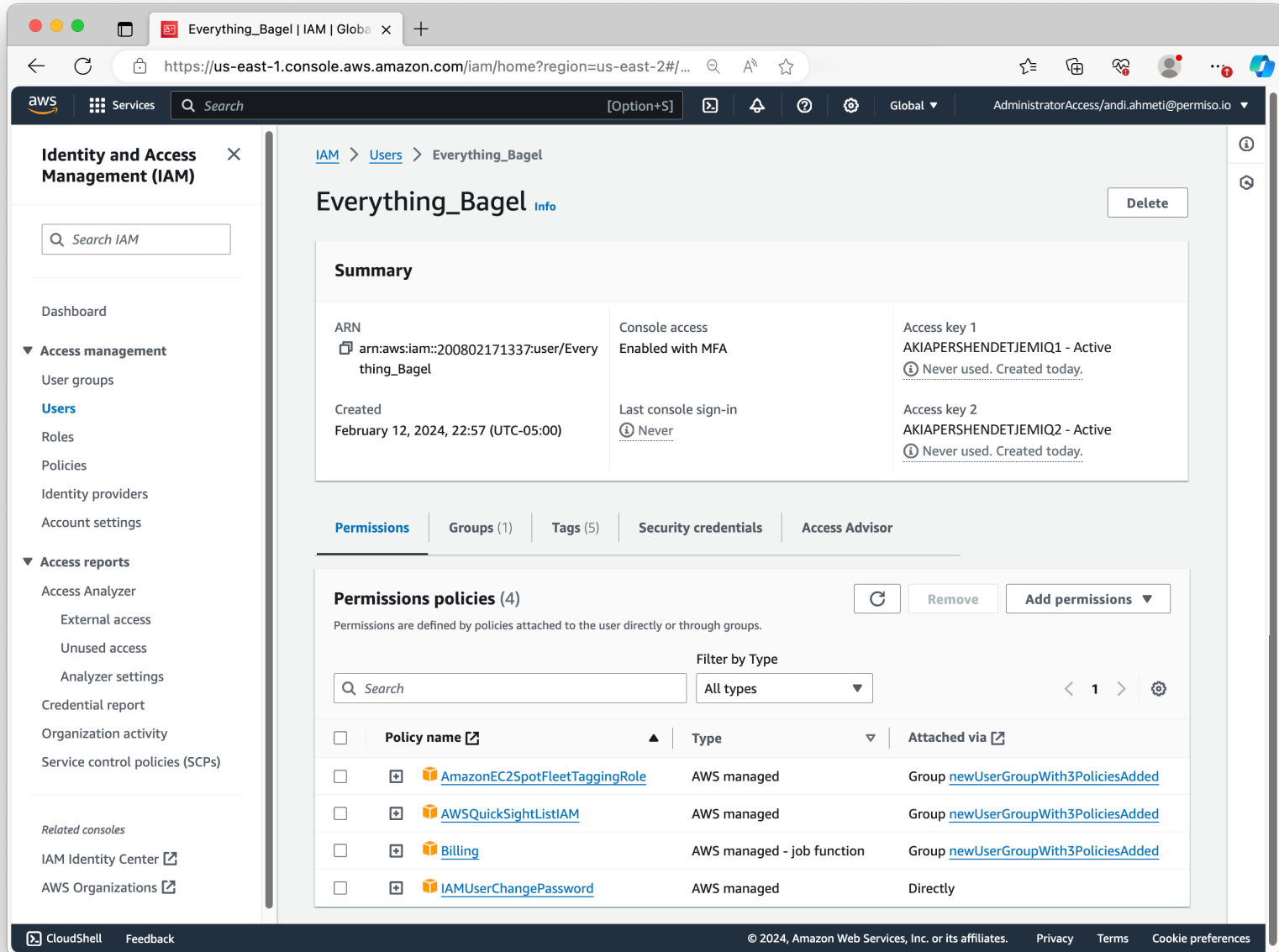


EVERYTHING_BAGEL



PLAIN_BAGEL

Console Mapping – Optional Events (Context)



The screenshot displays the AWS IAM console interface. The left-hand navigation pane is titled "Identity and Access Management (IAM)" and includes sections for "Access management" (User groups, Users, Roles, Policies, Identity providers, Account settings) and "Access reports" (Access Analyzer, Credential report, Organization activity, Service control policies (SCPs)).

The main content area shows the details for a user named "Everything_Bagel". The breadcrumb navigation is "IAM > Users > Everything_Bagel". A "Delete" button is visible in the top right corner.

Summary

ARN arn:aws:iam::200802171337:user/Everything_Bagel	Console access Enabled with MFA	Access key 1 AKIAPERSHENDETJEMIQ1 - Active Never used. Created today.
Created February 12, 2024, 22:57 (UTC-05:00)	Last console sign-in Never	Access key 2 AKIAPERSHENDETJEMIQ2 - Active Never used. Created today.

Below the summary, there are tabs for "Permissions", "Groups (1)", "Tags (5)", "Security credentials", and "Access Advisor". The "Permissions" tab is active, showing "Permissions policies (4)".

Permissions are defined by policies attached to the user directly or through groups.

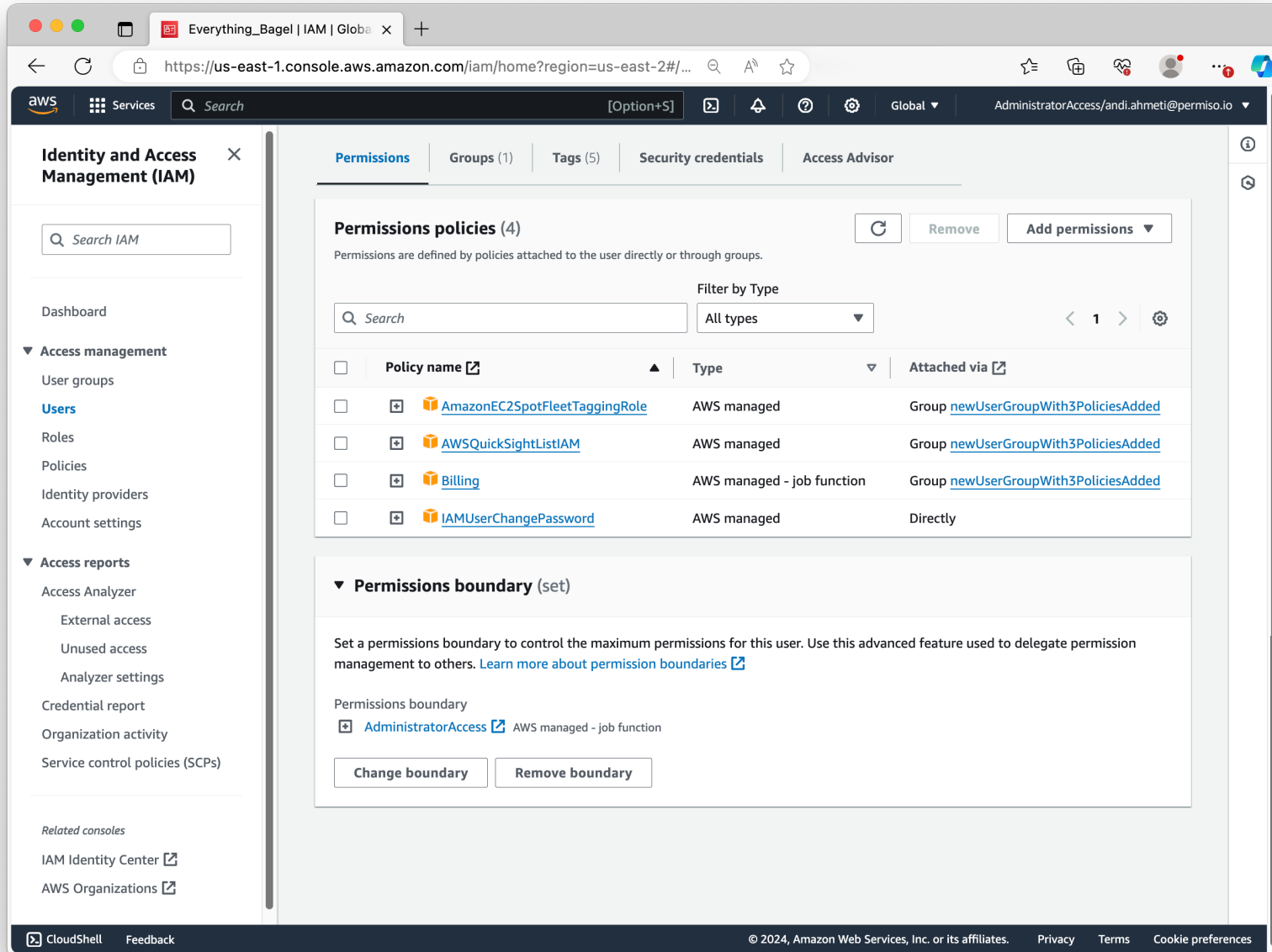
Filter by Type: All types

Policy name	Type	Attached via
AmazonEC2SpotFleetTaggingRole	AWS managed	Group newUserGroupWith3PoliciesAdded
AWSQuickSightListIAM	AWS managed	Group newUserGroupWith3PoliciesAdded
Billing	AWS managed - job function	Group newUserGroupWith3PoliciesAdded
IAMUserChangePassword	AWS managed	Directly

At the bottom of the console, there are links for "CloudShell" and "Feedback", and a footer with "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".



Console Mapping – OptionalEvents (Context)



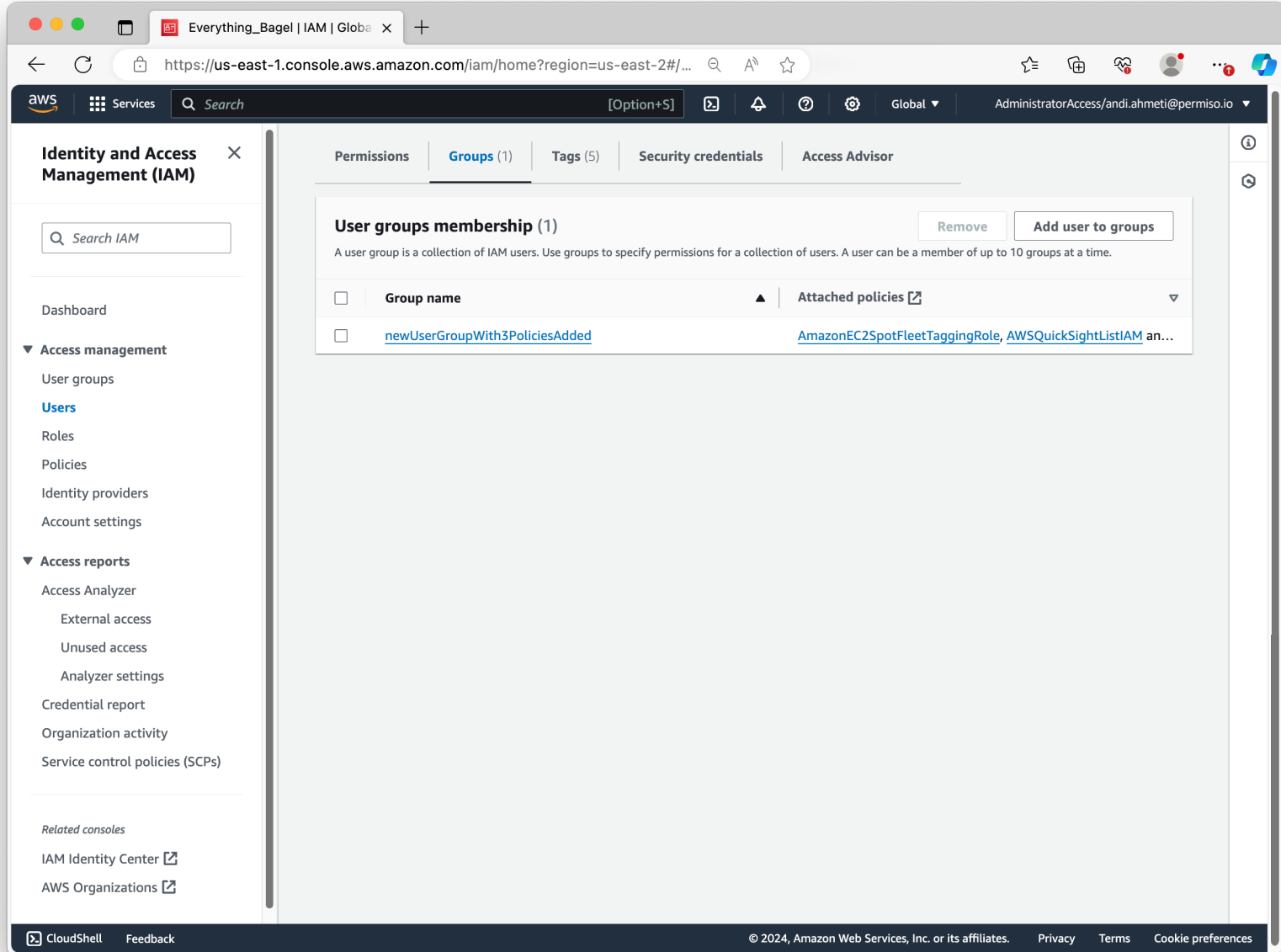
The screenshot displays the AWS IAM console interface. The left sidebar shows the navigation menu with sections for Access management (Users, Roles, Policies, Identity providers, Account settings) and Access reports (Access Analyzer, Credential report, Organization activity, Service control policies (SCPs)). The main content area is titled "Permissions policies (4)" and lists the following policies:

Policy name	Type	Attached via
AmazonEC2SpotFleetTaggingRole	AWS managed	Group newUserGroupWith3PoliciesAdded
AWSQuickSightListIAM	AWS managed	Group newUserGroupWith3PoliciesAdded
Billing	AWS managed - job function	Group newUserGroupWith3PoliciesAdded
IAMUserChangePassword	AWS managed	Directly

Below the policies, the "Permissions boundary (set)" section is visible, showing a boundary named "AdministratorAccess" (AWS managed - job function) with "Change boundary" and "Remove boundary" buttons.



Console Mapping – Optional Events (Context)



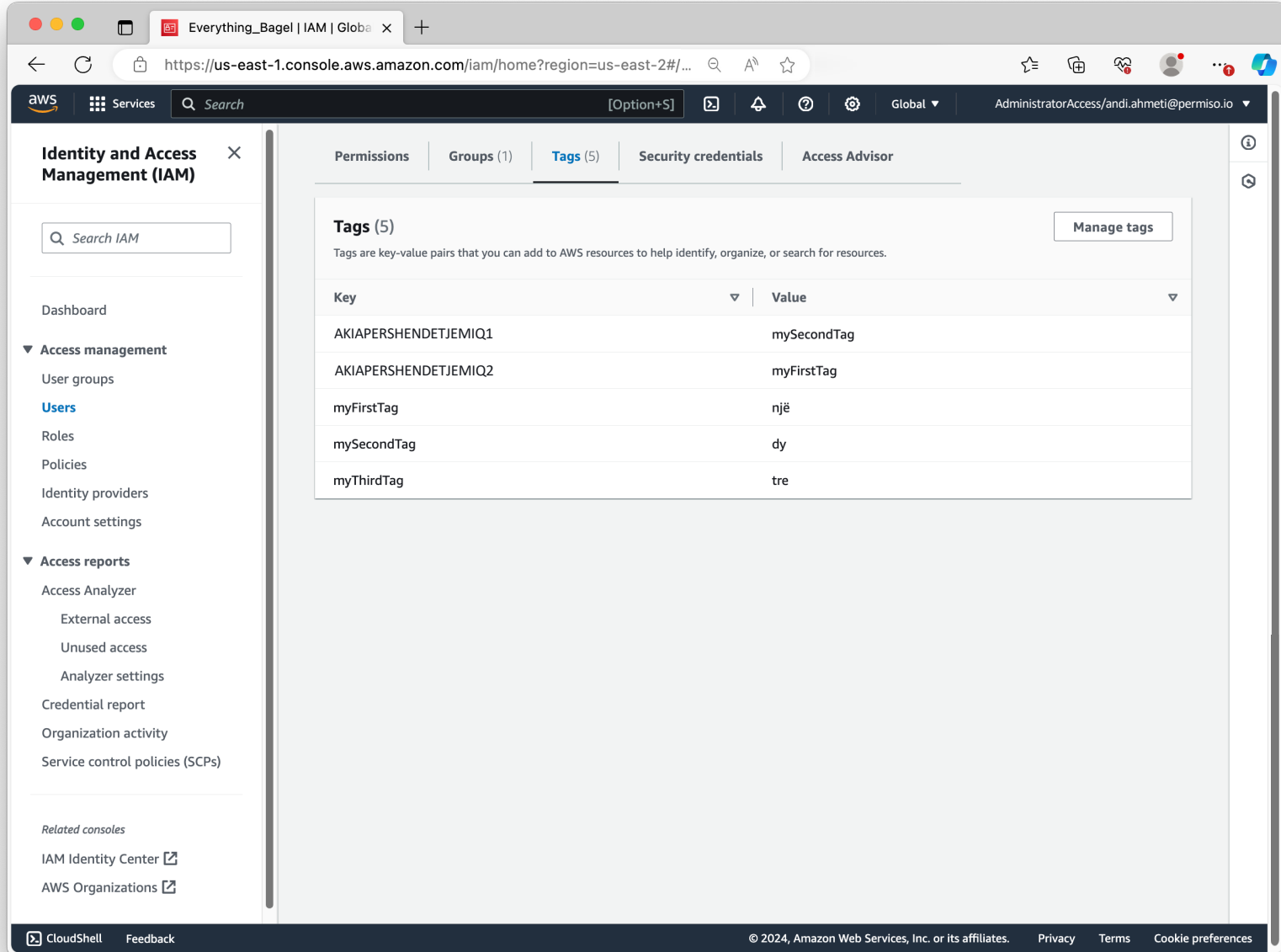
The screenshot displays the AWS IAM console interface. The left-hand navigation pane is titled "Identity and Access Management (IAM)" and includes a search bar and a menu with categories like "Access management" (containing User groups, Users, Roles, Policies, Identity providers, Account settings) and "Access reports" (containing Access Analyzer, Credential report, Organization activity, Service control policies (SCPs)). The main content area is titled "User groups membership (1)" and features a table with the following data:

<input type="checkbox"/>	Group name	Attached policies
<input type="checkbox"/>	newUserGroupWith3PoliciesAdded	AmazonEC2SpotFleetTaggingRole , AWSQuickSightListIAM an...

At the bottom of the console, there are links for "CloudShell" and "Feedback", and a footer with copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".



Console Mapping – OptionalEvents (Context)



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options for Identity and Access Management (IAM), including Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, Credential report, Organization activity, Service control policies), and Related consoles (IAM Identity Center, AWS Organizations). The main content area is titled 'Tags (5)' and displays a table of tags for the user 'AKIAPERSHENDETJEMIQ1'. The table has two columns: 'Key' and 'Value'. The tags listed are: mySecondTag, myFirstTag, një, dy, and tre. A 'Manage tags' button is visible in the top right corner of the table area.

Key	Value
AKIAPERSHENDETJEMIQ1	mySecondTag
AKIAPERSHENDETJEMIQ2	myFirstTag
myFirstTag	një
mySecondTag	dy
myThirdTag	tre



Console Mapping – Optional Events (Context)

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation options: Identity and Access Management (IAM), Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies (SCPs)), and Related consoles (IAM Identity Center, AWS Organizations).

The main content area is titled "Security credentials" and includes the following sections:

- Console sign-in:** Shows the console sign-in link (<https://200802171337signin.aws.amazon.com/console>), console password (updated 2 hours ago), and last console sign-in (Never).
- Multi-factor authentication (MFA) (1):** Includes buttons for Remove, Resync, and Assign MFA device. A table lists the MFA device:

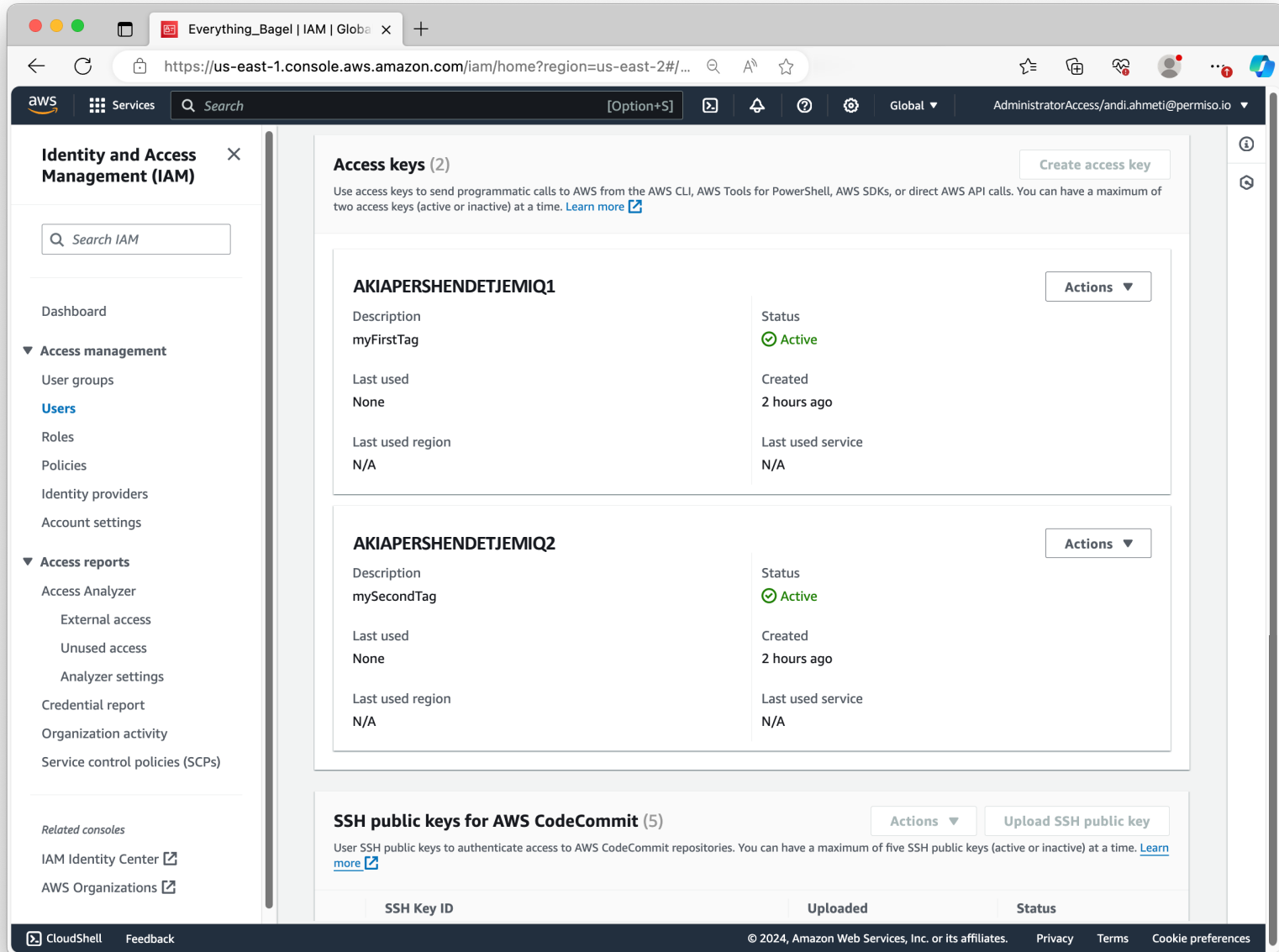
Device type	Identifier	Certifications	Created on
Virtual	arn:aws:iam::200802171337:mfa/ExampleMFADevice	Not Applicable	2 hours ago

- Access keys (2):** Includes a Create access key button. A table lists the access keys:

Access Key ID	Description	Status	Created
AKIAPERSHENDETJEMIQ1	myFirstTag	Active	2 hours ago



Console Mapping – Optional Events (Context)

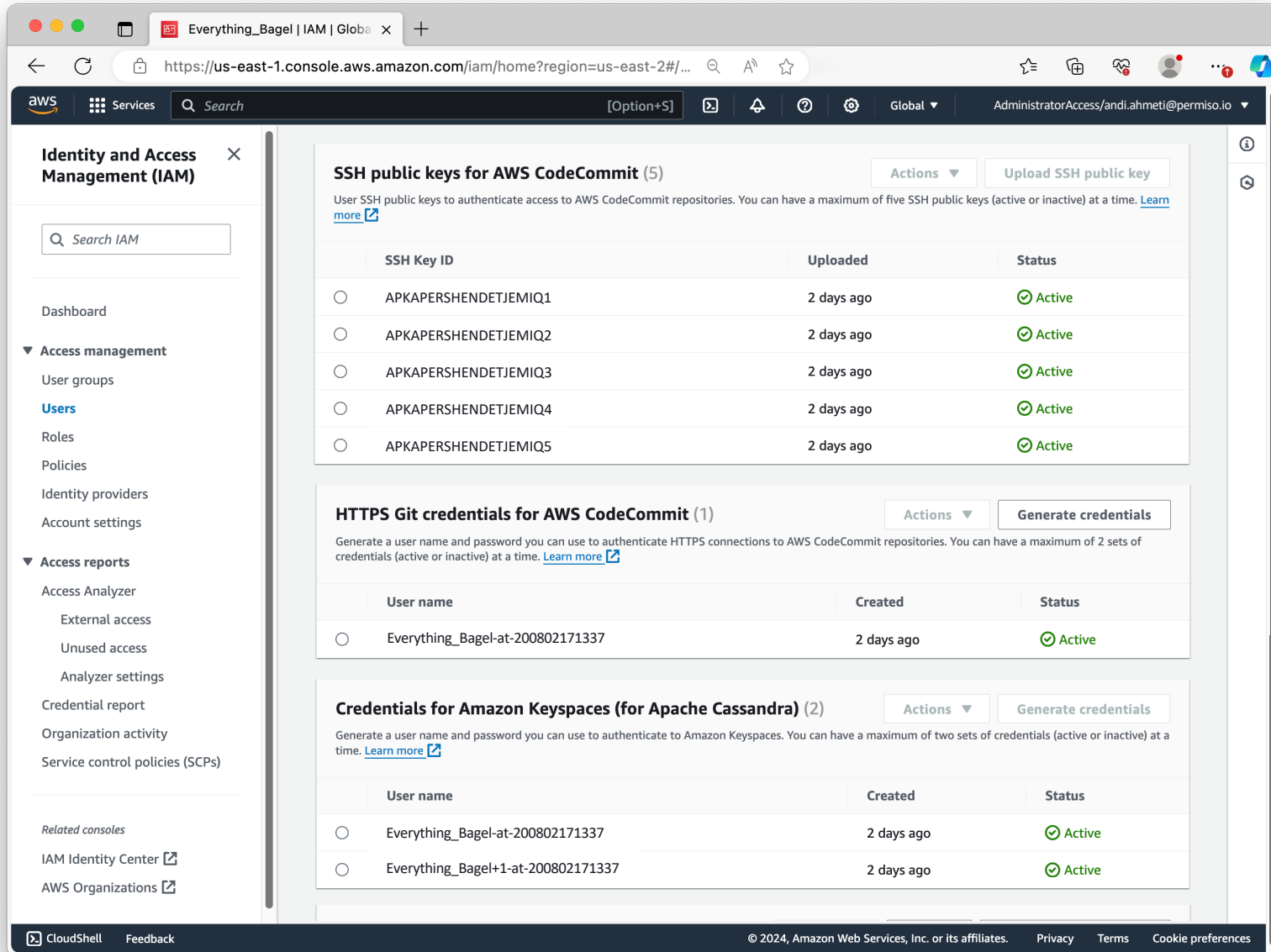


The screenshot displays the AWS IAM console interface. The left sidebar contains navigation options: Identity and Access Management (IAM), Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies (SCPs)), and Related consoles (IAM Identity Center, AWS Organizations). The main content area is titled 'Access keys (2)' and lists two active keys: AKIAPERSHENDETJEMIQ1 (myFirstTag) and AKIAPERSHENDETJEMIQ2 (mySecondTag). Both keys are active and were created 2 hours ago. Below this, there is a section for 'SSH public keys for AWS CodeCommit (5)'. The footer includes 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.

SSH Key ID	Uploaded	Status
AKIAPERSHENDETJEMIQ1	myFirstTag	Active
AKIAPERSHENDETJEMIQ2	mySecondTag	Active



Console Mapping – Optional Events (Context)



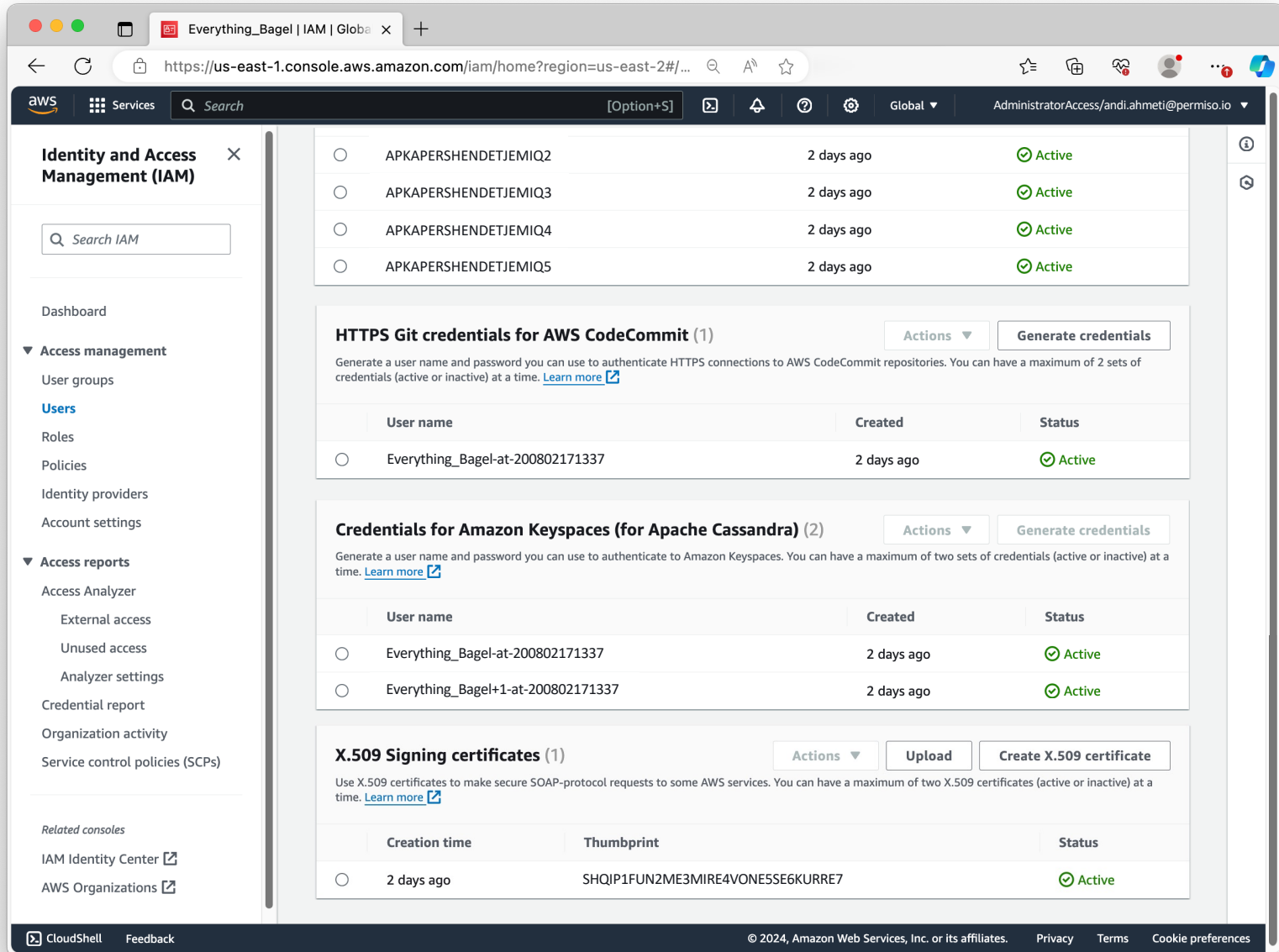
The screenshot displays the AWS IAM console interface. The left sidebar shows the navigation menu for Identity and Access Management (IAM), including sections for Access management (Users, Roles, Policies, Identity providers, Account settings) and Access reports (Access Analyzer, Credential report, Organization activity, Service control policies). The main content area is divided into three sections:

- SSH public keys for AWS CodeCommit (5)**: A table listing five active SSH keys, each uploaded 2 days ago. The keys are identified by IDs starting with 'APKAPERSHENDETJEMIQ'.
- HTTPS Git credentials for AWS CodeCommit (1)**: A table showing one active credential with the user name 'Everything_Bagel-at-200802171337', created 2 days ago.
- Credentials for Amazon Keyspaces (for Apache Cassandra) (2)**: A table showing two active credentials with user names 'Everything_Bagel-at-200802171337' and 'Everything_Bagel+1-at-200802171337', both created 2 days ago.

The footer of the console includes 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for Privacy, Terms, and Cookie preferences.



Console Mapping – Optional Events (Context)



The screenshot displays the AWS IAM console interface. The left sidebar contains navigation options: Identity and Access Management (IAM), Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies (SCPs)), and Related consoles (IAM Identity Center, AWS Organizations).

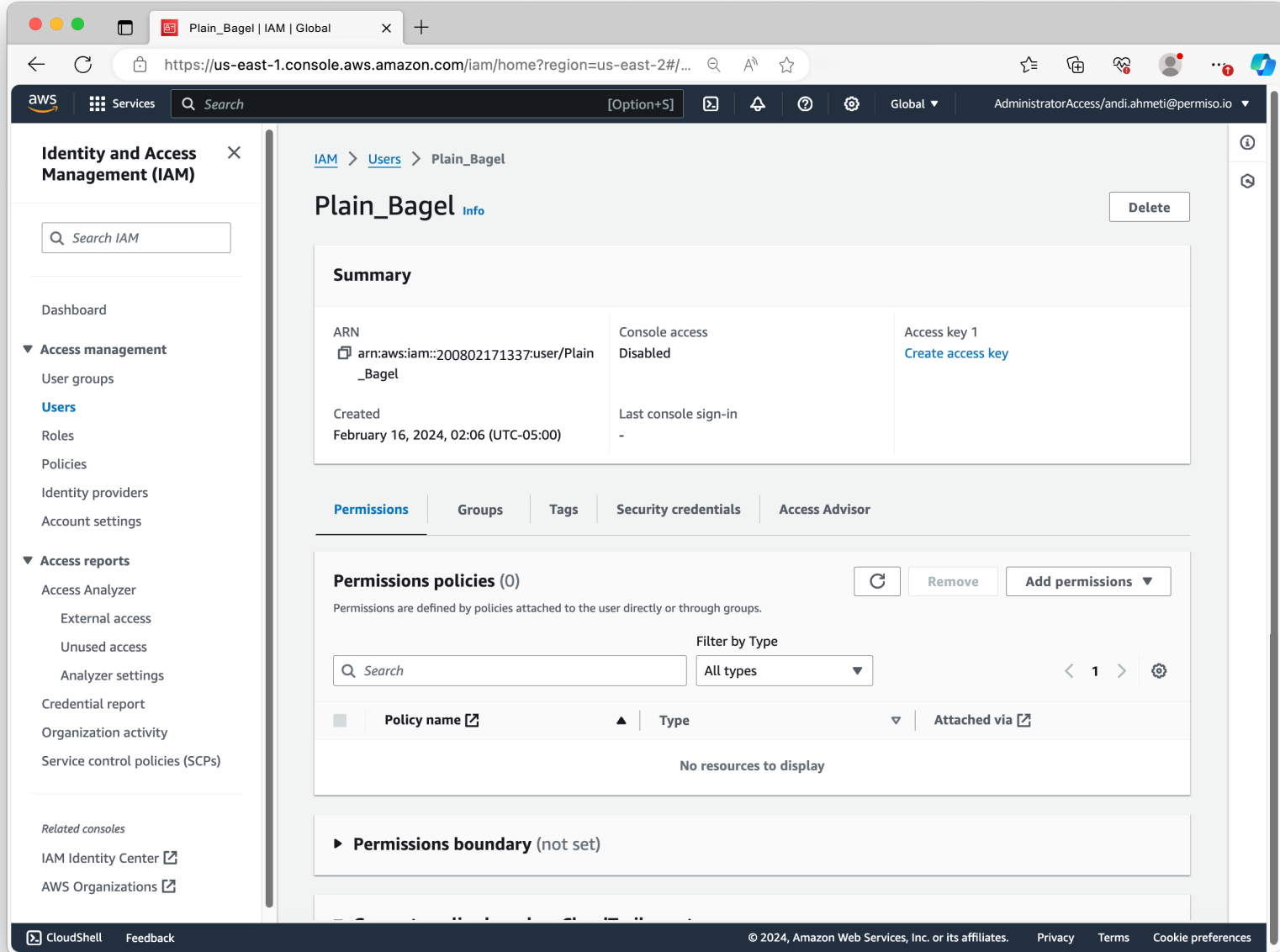
The main content area is divided into several sections:

- Users:** A table listing five users with IDs APKAPERSHENDETJEMIQ2 through Q5, all created 2 days ago and in an Active state.
- HTTPS Git credentials for AWS CodeCommit (1):** A section with an "Actions" dropdown and a "Generate credentials" button. Below is a table with one entry: "Everything_Bagel-at-200802171337", created 2 days ago, and Active.
- Credentials for Amazon Keyspaces (for Apache Cassandra) (2):** A section with an "Actions" dropdown and a "Generate credentials" button. Below is a table with two entries: "Everything_Bagel-at-200802171337" and "Everything_Bagel+1-at-200802171337", both created 2 days ago and Active.
- X.509 Signing certificates (1):** A section with an "Actions" dropdown, an "Upload" button, and a "Create X.509 certificate" button. Below is a table with one entry: created 2 days ago, with thumbprint SHQP1FUN2ME3MIRE4VONE5SE6KURRE7, and Active.

The footer of the console shows "CloudShell", "Feedback", and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for Privacy, Terms, and Cookie preferences.



Console Mapping – OptionalEvents (Context)



The screenshot displays the AWS IAM console interface. The left-hand navigation pane is titled "Identity and Access Management (IAM)" and includes sections for "Access management" (User groups, Users, Roles, Policies, Identity providers, Account settings) and "Access reports" (Access Analyzer, Credential report, Organization activity, Service control policies (SCPs)). The main content area shows the details for a user named "Plain_Bagel".

Plain_Bagel Info Info Delete

Summary

ARN arn:aws:iam::200802171337:user/Plain_Bagel	Console access Disabled	Access key 1 Create access key
Created February 16, 2024, 02:06 (UTC-05:00)	Last console sign-in -	

Permissions | Groups | Tags | Security credentials | Access Advisor

Permissions policies (0) Refresh Remove Add permissions

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
Search: All types < 1 > Settings

Policy name	Type	Attached via
No resources to display		

Permissions boundary (not set)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

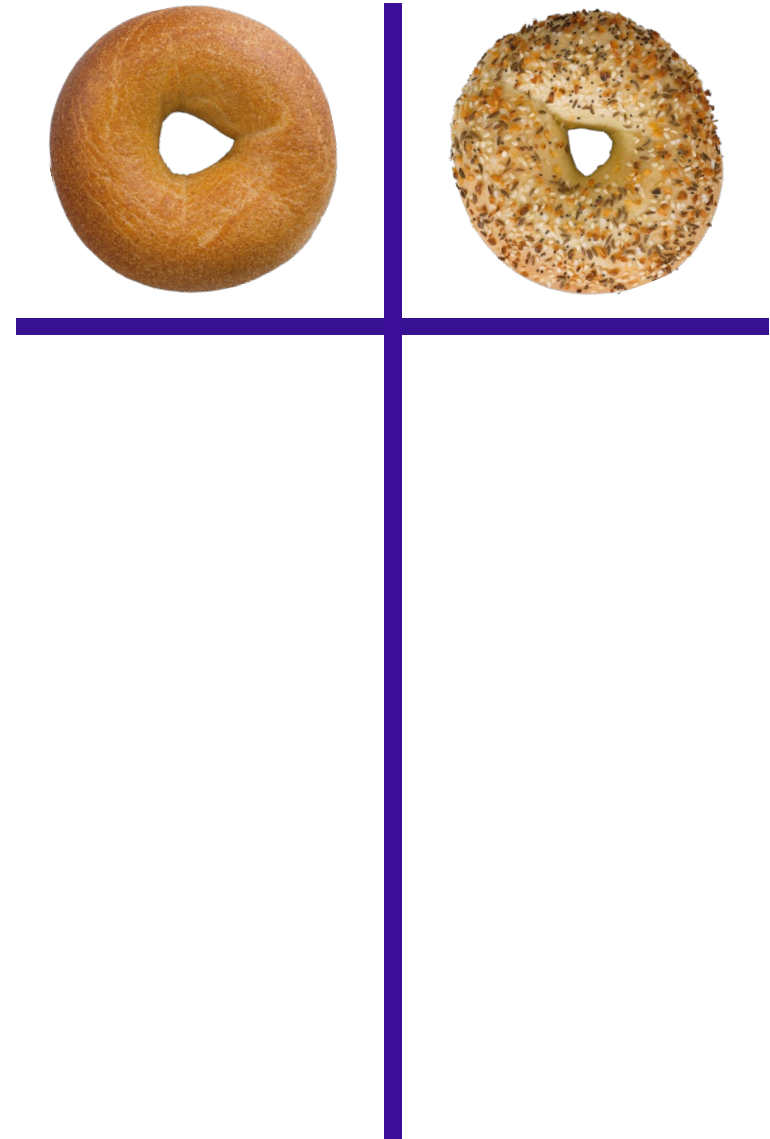


Console Mapping – OptionalEvents (Context)

The screenshot shows the AWS IAM console interface. The browser address bar indicates the URL: `https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#...`. The page title is "Plain_Bagel | IAM | Global". The main content area displays the "Plain_Bagel" user details, including a summary table with the following information:

Summary		
ARN <code>arn:aws:iam::200802171337:user/Plain_Bagel</code>	Console access Disabled	Access key 1 Create access key
Created February 16, 2024, 02:06 (UTC-05:00)	Last console sign-in -	

Below the summary, there are tabs for "Permissions", "Groups", "Tags", "Security credentials", and "Access Advisor". The "Permissions" tab is active, showing "Permissions policies (0)". A search bar and a "Filter by Type" dropdown (set to "All types") are present. Below this, a table header is visible with columns for "Policy name", "Type", and "Attached via". The table currently displays "No resources to display".



Console Mapping – Optional Events (Context)



Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------

eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:21:20.0000	iam:GetUser	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:21:20.0000	iam:ListMFADevices	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:21:20.0000	iam:ListUserTags	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:21:20.0000	iam:ListUserPolicies	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:21:20.0000	iam:ListAttachedUserPolicies	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:21:20.0000	iam:ListPolicies	AWS Internal	{"maxItems":1000,"onlyAttached":false}
2024-03-18 04:21:24.0000	iam:ListPolicies	AWS Internal	{"maxItems":1000,"marker":"AAI1zjUVInJUxBcsOtgybPoPxBF..."}
2024-03-18 04:21:21.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Plain_Bagel"}
2024-03-18 04:21:21.0000	access-analyzer:ListPolicyGenerations	aws-internal/3 aws-sdk-java/...	{"principalArn":"arn:aws:iam::200802171337:user/Plain_Bagel"}
2024-03-18 04:21:20.0000	iam:ListAccessKeys	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:21:21.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Plain_Bagel"}

Console Mapping – Optional Events (Context)



Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------

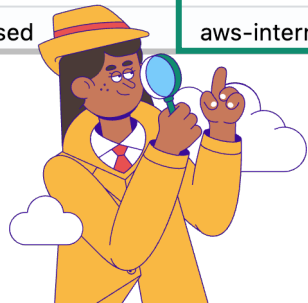
eventTime	eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:GetUser	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListMFADevices	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListUserTags	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListUserPolicies	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListAttachedUserPolicies	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:GetPolicy	AWS Internal	{"policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"}
2024-03-18 04:21:24.0000	2024-03-18 04:24:43.0000	iam:ListGroupPolicies	AWS Internal	{"groupName":"customGroup2"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:ListAttachedGroupPolicies	AWS Internal	{"groupName":"customGroup2"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	access-analyzer:ListPolicyGenerations	aws-internal/3 aws-sdk-java/...	{"principalArn":"arn:aws:iam::200802171337:user/Everything_Bagel"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:ListAccessKeys	AWS Internal	{"userName":"Everything_Bagel"}
	2024-03-18 04:24:44.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Everything_Bagel"}
	2024-03-18 04:24:44.0000	iam:GetAccessKeyLastUsed	AWS Internal	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:44.0000	iam:GetAccessKeyLastUsed	AWS Internal	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}
	2024-03-18 04:24:45.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:45.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}

Console Mapping – OptionalEvents (Context)



- Permissions
- Groups
- Tags
- Security credentials
- Access Advisor

eventTime	eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:GetUser	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListMFADevices	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListUserTags	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListUserPolicies	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListAttachedUserPolicies	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:GetPolicy	AWS Internal	{"policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"}
2024-03-18 04:21:24.0000	2024-03-18 04:24:43.0000	iam:ListGroupPolicies	AWS Internal	{"groupName":"customGroup2"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:ListAttachedGroupPolicies	AWS Internal	{"groupName":"customGroup2"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	access-analyzer:ListPolicyGenerations	aws-internal/3 aws-sdk-java/...	{"principalArn":"arn:aws:iam::200802171337:user/Everything_Bagel"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:ListAccessKeys	AWS Internal	{"userName":"Everything_Bagel"}
	2024-03-18 04:24:44.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Everything_Bagel"}
	2024-03-18 04:24:44.0000	iam:GetAccessKeyLastUsed	AWS Internal	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:44.0000	iam:GetAccessKeyLastUsed	AWS Internal	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}
	2024-03-18 04:24:45.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:45.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}



Console Mapping – Optional Events (Context)



Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------

eventTime	eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:GetUser	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListMFADevices	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListUserTags	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListUserPolicies	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:ListAttachedUserPolicies	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	iam:GetPolicy	AWS Internal	{"policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"}
2024-03-18 04:21:24.0000	2024-03-18 04:24:43.0000	iam:ListGroupPolicies	AWS Internal	{"groupName":"customGroup2"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:ListAttachedGroupPolicies	AWS Internal	{"groupName":"customGroup2"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	access-analyzer:ListPolicyGenerations	aws-internal/3 aws-sdk-java/...	{"principalArn":"arn:aws:iam::200802171337:user/Everything_Bagel"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:ListAccessKeys	AWS Internal	{"userName":"Everything_Bagel"}
	2024-03-18 04:24:44.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Everything_Bagel"}
	2024-03-18 04:24:44.0000	iam:GetAccessKeyLastUsed	AWS Internal	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:44.0000	iam:GetAccessKeyLastUsed	AWS Internal	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}
	2024-03-18 04:24:45.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:45.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}

Console Mapping – OptionalEvents (Context)



Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------

eventNameFull	☰
iam:GetUser	
iam:ListMFADevices	
iam:ListUserTags	
iam:ListUserPolicies	
iam:ListAttachedUserPolicies	
iam:ListPolicies	
iam:ListPolicies	
iam:GetLoginProfile	
access-analyzer:ListPolicyGenerations	
iam:ListAccessKeys	
iam:ListAccessKeys	

eventNameFull	☰
iam:GetUser	
iam:ListMFADevices	
iam:ListUserTags	
iam:ListUserPolicies	
iam:ListAttachedUserPolicies	
iam:GetPolicy	
iam:ListGroupPolicies	
iam:ListAttachedGroupPolicies	
iam:GetLoginProfile	
access-analyzer:ListPolicyGenerations	
iam:ListAccessKeys	
iam:ListAccessKeys	
iam:GetAccessKeyLastUsed	
iam:GetAccessKeyLastUsed	
iam:GetAccessKeyLastUsed	
iam:GetAccessKeyLastUsed	

Console Mapping – Optional Events (Context)



Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------

eventNameFull		eventNameFull	
iam:GetUser		iam:GetUser	
iam:ListMFADevices		iam:ListMFADevices	
iam:ListUserTags		iam:ListUserTags	
iam:ListUserPolicies		iam:ListUserPolicies	
iam:ListAttachedUserPolicies		iam:ListAttachedUserPolicies	

iam:ListPolicies
iam:ListPolicies

iam:GetPolicy
iam:ListGroupPolicies
iam:ListAttachedGroupPolicies

iam:GetLoginProfile	iam:GetLoginProfile
access-analyzer:ListPolicyGenerations	access-analyzer:ListPolicyGenerations
iam:ListAccessKeys	iam:ListAccessKeys
iam:ListAccessKeys	iam:ListAccessKeys

iam:GetAccessKeyLastUsed
iam:GetAccessKeyLastUsed
iam:GetAccessKeyLastUsed
iam:GetAccessKeyLastUsed

Console Mapping – Optional Events (Context)



iam:ListPolicies

Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------

eventNameFull	☰
iam:GetUser	
iam:ListMFADevices	
iam:ListUserTags	
iam:ListUserPolicies	
iam:ListAttachedUserPolicies	

eventNameFull	☰
iam:GetUser	
iam:ListMFADevices	
iam:ListUserTags	
iam:ListUserPolicies	
iam:ListAttachedUserPolicies	

iam:GetLoginProfile
access-analyzer:ListPolicyGenerations
iam:ListAccessKeys
iam:ListAccessKeys

iam:GetLoginProfile
access-analyzer:ListPolicyGenerations
iam:ListAccessKeys
iam:ListAccessKeys



iam:GetPolicy
iam:ListGroupPolicies
iam:ListAttachedGroupPolicies
iam:GetAccessKeyLastUsed

Console Mapping – Optional Events (Context)



iam:ListPolicies

Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------



iam:GetPolicy
iam:ListGroupPolicies
iam:ListAttachedGroupPolicies
iam:GetAccessKeyLastUsed

eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:23:04.0000	iam:ListAccessKeys	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:23:04.0000	iam:ListSigningCertificates	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:23:04.0000	iam:ListSSHPublicKeys	AWS Internal	{"userName":"Plain_Bagel"}
2024-03-18 04:23:04.0000	iam:ListServiceSpecificCredentials	AWS Internal	{"userName":"Plain_Bagel","serviceName":"cassandra.amazonaw..."}
2024-03-18 04:23:04.0000	iam:ListServiceSpecificCredentials	AWS Internal	{"userName":"Plain_Bagel","serviceName":"codecommit.amazona..."}

eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:25:29.0000	iam:ListAccessKeys	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:25:29.0000	iam:ListSigningCertificates	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:25:29.0000	iam:ListSSHPublicKeys	AWS Internal	{"userName":"Everything_Bagel"}
2024-03-18 04:25:29.0000	iam:ListServiceSpecificCredentials	AWS Internal	{"userName":"Everything_Bagel","serviceName":"cassandra.ama..."}
2024-03-18 04:25:29.0000	iam:ListServiceSpecificCredentials	AWS Internal	{"userName":"Everything_Bagel","serviceName":"codecommit.am..."}
2024-03-18 04:25:29.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
2024-03-18 04:25:29.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}

Console Mapping – Optional Events (Context)



iam:ListPolicies

Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	-----------------------------	----------------

eventNameFull	☰
iam:ListAccessKeys	
iam:ListSigningCertificates	
iam:ListSSHPublicKeys	
iam:ListServiceSpecificCredentials	
iam:ListServiceSpecificCredentials	

eventNameFull	☰
iam:ListAccessKeys	
iam:ListSigningCertificates	
iam:ListSSHPublicKeys	
iam:ListServiceSpecificCredentials	
iam:ListServiceSpecificCredentials	
iam:GetAccessKeyLastUsed	
iam:GetAccessKeyLastUsed	



iam:GetPolicy
iam:ListGroupPolicies
iam:ListAttachedGroupPolicies
iam:GetAccessKeyLastUsed

Console Mapping – Optional Events (Context)



iam:ListPolicies

Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------

eventNameFull		eventNameFull	
iam:ListAccessKeys		iam:ListAccessKeys	
iam:ListSigningCertificates		iam:ListSigningCertificates	
iam:ListSSHPublicKeys		iam:ListSSHPublicKeys	
iam:ListServiceSpecificCredentials		iam:ListServiceSpecificCredentials	
iam:ListServiceSpecificCredentials		iam:ListServiceSpecificCredentials	

iam:GetAccessKeyLastUsed
iam:GetAccessKeyLastUsed



iam:GetPolicy
iam:ListGroupPolicies
iam:ListAttachedGroupPolicies
iam:GetAccessKeyLastUsed

Console Mapping – Optional Events (Context)



iam:ListPolicies

Permissions	Groups	Tags	Security credentials	Access Advisor
-------------	--------	------	----------------------	----------------

eventNameFull		eventNameFull	
iam:ListAccessKeys		iam:ListAccessKeys	
iam:ListSigningCertificates		iam:ListSigningCertificates	
iam:ListSSHPublicKeys		iam:ListSSHPublicKeys	
iam:ListServiceSpecificCredentials		iam:ListServiceSpecificCredentials	
iam:ListServiceSpecificCredentials		iam:ListServiceSpecificCredentials	



iam:GetPolicy
iam:ListGroupPolicies
iam:ListAttachedGroupPolicies
iam:GetAccessKeyLastUsed

CLI vs Console

STEP COUNTER



CLI vs Console



```
bash-3.2$  
bash-3.2$ aws iam create-user --user-name krileva  
{  
  "User": {  
    "Path": "/",  
    "UserName": "krileva",  
    "UserId": "AIDA12345678ABCDEFGHI",  
    "Arn": "arn:aws:iam::200802171337:user/krileva",  
    "CreateDate": "2024-03-22T03:48:59+00:00"  
  }  
}  
bash-3.2$  
bash-3.2$ aws iam create-access-key --user-name krileva  
{  
  "AccessKey": {  
    "UserName": "krileva",  
    "AccessKeyId": "AKIA12345678ABCDEFGH",  
    "Status": "Active",  
    "SecretAccessKey": "SHQIP1337PunaEshteShendet4U+po+iRedacted",  
    "CreateDate": "2024-03-22T03:49:17+00:00"  
  }  
}  
bash-3.2$  
bash-3.2$ aws iam attach-user-policy --user-name krileva \  
> --policy-arn arn:aws:iam::aws:policy/AdministratorAccess  
bash-3.2$
```

CLI vs Console



```
bash-3.2$  
bash-3.2$ aws iam create-user --user-name krileva  
{  
  "User": {  
    "Path": "/",  
    "UserName": "krileva",  
    "UserId": "AIDA12345678ABCDEFGHI",  
    "Arn": "arn:aws:iam::200802171337:user/krileva",  
    "CreateDate": "2024-03-22T03:48:59+00:00"  
  }  
}  
bash-3.2$  
bash-3.2$ aws iam create-access-key --user-name krileva  
{  
  "AccessKey": {  
    "UserName": "krileva",  
    "AccessKeyId": "AKIA12345678ABCDEFGH",  
    "Status": "Active",  
    "SecretAccessKey": "SHQIP1337PunaEshteShendet4U+po+iRedacted",  
    "CreateDate": "2024-03-22T03:49:17+00:00"  
  }  
}  
bash-3.2$  
bash-3.2$ aws iam attach-user-policy --user-name krileva \  
> --policy-arn arn:aws:iam::aws:policy/AdministratorAccess  
bash-3.2$
```

1

2

3

CLI vs Console



```
bash-3.2$ aws iam create-user --user-name krileva
{
  "User": {
    "Path": "/",
    "UserName": "krileva",
    "UserId": "AIDA12345678ABCDEFGHI",
    "Arn": "arn:aws:iam::200802171337:user/krileva",
    "CreateDate": "2024-03-22T03:48:59+00:00"
  }
}
bash-3.2$ aws iam create-access-key --user-name krileva
{
  "AccessKey": {
    "UserName": "krileva",
    "AccessKeyId": "AKIA12345678ABCDEFGH",
    "Status": "Active",
    "SecretAccessKey": "SHQIP1337PunaEshteShendet4U+po+iRedacted",
    "CreateDate": "2024-03-22T03:49:17+00:00"
  }
}
bash-3.2$ aws iam attach-user-policy --user-name krileva \
> --policy-arn arn:aws:iam::aws:policy/AdministratorAccess
```

1

2

3

eventNameFull	requestParameters
iam:CreateUser	{"userName":"krileva"}
iam:CreateAccessKey	{"userName":"krileva"}
iam:AttachUserPolicy	{"userName":"krileva","policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"}

eventCount	userAgent
1	aws-cli/2.13.0 Python/3.11.4 Darwin/22.6.0 source/arm64 prompt/off command iam.create-user
1	aws-cli/2.13.0 Python/3.11.4 Darwin/22.6.0 source/arm64 prompt/off command iam.create-access-key
1	aws-cli/2.13.0 Python/3.11.4 Darwin/22.6.0 source/arm64 prompt/off command iam.attach-user-policy

CLI vs Console



```
bash-3.2$  
bash-3.2$ python3 ./temp.py  
  
iam_client.create_user(Username=krileva) 1  
  
{'Arn': 'arn:aws:iam::200802171337:user/krileva',  
'CreateDate': datetime.datetime(2024, 3, 22, 4, 52, 49, tzinfo=tzutc()),  
'Path': '/',  
'UserId': 'AIDA12345678ABCDEFGHI',  
'UserName': 'krileva'}  
  
iam_client.create_access_key(Username=krileva) 2  
  
{'AccessKeyId': 'AKIA12345678ABCDEFGH',  
'CreateDate': datetime.datetime(2024, 3, 22, 4, 52, 49, tzinfo=tzutc()),  
'SecretAccessKey': 'SHQIP1337PunaEshteShendet4U+po+iRedacted',  
'Status': 'Active',  
'UserName': 'krileva'} 3  
  
iam_client.attach_user_policy(Username=krileva,PolicyArn=arn:aws:iam::aws:  
policy/AdministratorAccess)  
  
bash-3.2$
```

```
1 import boto3  
2 from pprint import pprint  
3  
4 # Define IAM client  
5 iam_client = boto3.client('iam')  
6  
7 # Specify username for new IAM User  
8 username = 'krileva'  
9  
10 # Specify policy ARN to add to newly created IAM User  
11 policyArn = "arn:aws:iam::aws:policy/AdministratorAccess"  
12  
13 # Create IAM User 1  
14 response = iam_client.create_user(Username=username)  
15 print(f"\niam_client.create_user(Username={username})\n")  
16 pprint (response['User'])  
17  
18 # Create Access Key for newly created IAM User 2  
19 response = iam_client.create_access_key(Username=username)  
20 print(f"\niam_client.create_access_key(Username={username})\n")  
21 pprint (response['AccessKey'])  
22  
23 # Attach policy to newly created IAM User 3  
24 response = iam_client.attach_user_policy(Username=username,PolicyArn=policyArn)  
25 print(f"\niam_client.attach_user_policy(Username={username},PolicyArn={policyArn})\n")  
26
```


CLI vs Console

eventCount	userAgent
3	Boto3/1.28.27 md/Botocore#1.31.27 ua/2.0 os/macos#22.6.0 md/arch#arm64 lang/python#3.11.4 md/pyimpl#CPython cfg/retry-mode#legacy Botocore/1.31.27

```
bash-3.2$ python3 ./temp.py

iam_client.create_user(Username=krileva)

{'Arn': 'arn:aws:iam::200802171337:user/krileva',
 'CreateDate': datetime.datetime(2024, 3, 22, 4, 52, 49, tzinfo=tzutc()),
 'Path': '/',
 'UserId': 'AIDA12345678ABCDEFGHI',
 'UserName': 'krileva'}

iam_client.create_access_key(Username=krileva)

{'AccessKeyId': 'AKIA12345678ABCDEFGH',
 'CreateDate': datetime.datetime(2024, 3, 22, 4, 52, 49, tzinfo=tzutc()),
 'SecretAccessKey': 'SHQIP1337PunaEshteShendet4U+po+iRedacted',
 'Status': 'Active',
 'UserName': 'krileva'}

iam_client.attach_user_policy(Username=krileva, PolicyArn=arn:aws:iam::aws:policy/AdministratorAccess)

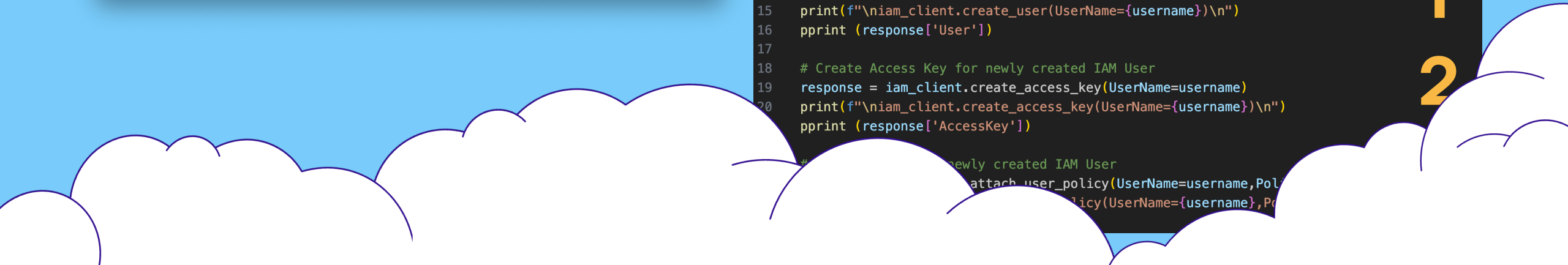
bash-3.2$
```

1
2
3

eventNameFull	requestParameters
iam:CreateUser	{"userName":"krileva"}
iam:CreateAccessKey	{"userName":"krileva"}
iam:AttachUserPolicy	{"userName":"krileva","policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"}

```
1 import boto3
2 from pprint import pprint
3
4 # Define IAM client
5 iam_client = boto3.client('iam')
6
7 # Specify username for new IAM User
8 username = 'krileva'
9
10 # Specify policy ARN to add to newly created IAM User
11 policyArn = "arn:aws:iam::aws:policy/AdministratorAccess"
12
13 # Create IAM User
14 response = iam_client.create_user(Username=username)
15 print(f"\niam_client.create_user(Username={username})\n")
16 pprint (response['User'])
17
18 # Create Access Key for newly created IAM User
19 response = iam_client.create_access_key(Username=username)
20 print(f"\niam_client.create_access_key(Username={username})\n")
21 pprint (response['AccessKey'])
22
23 # Attach policy to newly created IAM User
24 iam_client.attach_user_policy(Username=username, PolicyArn=policyArn)
25 print(f"\niam_client.attach_user_policy(Username={username}, PolicyArn={policyArn})\n")
26 pprint (response['Policy'])
```

1
2



CLI vs Console

A screenshot of the AWS IAM console interface. The browser address bar shows the URL: https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/. The page title is "Users | IAM | Global". The left-hand navigation pane is titled "Identity and Access Management (IAM)" and includes sections for "Access management" (User groups, Users, Roles, Policies, Identity providers, Account settings) and "Access reports" (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity). The main content area is titled "IAM > Users" and contains a "Users (3) Info" section with a "Create user" button. Below this is a table of users with columns for checkboxes, User name, Path, Groups, Last activity, MFA, and Password. The table lists three users: Andi_Ahmeti, Daniel_Bohannon, and No_Permissions.

<input type="checkbox"/>	User name	Path	Groups	Last activity	MFA	Password
<input type="checkbox"/>	Andi_Ahmeti	/	1	-	-	-
<input type="checkbox"/>	Daniel_Bohannon	/	1	-	-	-
<input type="checkbox"/>	No_Permissions	/	0	5 hours ago	Virtual	-

CLI vs Console



ConsoleHome

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:54:52.0000	servicecatalog-appregistry:ListApplications	Mozilla/5.0 (Macintosh; Intel ...	{"maxResults":"100"}
2024-03-22 04:54:52.0000	notifications:ListNotificationHubs	Mozilla/5.0 (Macintosh; Intel ...	
2024-03-22 04:54:52.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"eventTypeCategories":["scheduledChange...
2024-03-22 04:54:52.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"startTimes":[{"from":"Mar 15, 2024 4:54:5...
2024-03-22 04:54:52.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"startTimes":[{"from":"Mar 15, 2024 4:54:5...
2024-03-22 04:54:52.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"startTimes":[{"from":"Mar 15, 2024 4:54:5...
2024-03-22 04:54:52.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"startTimes":[{"from":"Mar 15, 2024, 4:54:5...
2024-03-22 04:54:52.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"startTimes":[{"from":"Mar 15, 2024, 4:54:5...
2024-03-22 04:54:53.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"eventStatusCodes":["open","upcoming"],"...
2024-03-22 04:54:53.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"startTimes":[{"from":"Mar 15, 2024 4:54:5...
2024-03-22 04:54:53.0000	ec2:DescribeRegions	Mozilla/5.0 (Macintosh; Intel ...	{"regionSet":{},"allRegions":true}
2024-03-22 04:54:53.0000	ce:GetCostForecast	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"Key":"RECOR...
2024-03-22 04:54:53.0000	ce:GetCostAndUsage	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":{"Dimensions":{"Key":"RECOR...

13

SearchBar

eventNameFull	requestParameters
	ATOR"}

1

CLI vs Console



SearchBar

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:55:05.0000	resource-explorer-2:ListIndexes	Mozilla/5.0 (Macintosh; Intel ...	{"Type":"AGGREGATOR"}

1

13

IAM_Dashboard

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:55:06.0000	organizations:DescribeOrganization	AWS Internal	
2024-03-22 04:55:06.0000	notifications:ListNotificationHubs	Mozilla/5.0 (Macintosh; Intel ...	
2024-03-22 04:55:06.0000	iam:ListMFADevices	AWS Internal	{"userName":"No_Permissions"}
2024-03-22 04:55:06.0000	iam:ListAccountAliases	AWS Internal	
2024-03-22 04:55:06.0000	iam:ListAccessKeys	AWS Internal	{"userName":"No_Permissions"}
2024-03-22 04:55:06.0000	iam:GetAccountSummary	AWS Internal	
2024-03-22 04:55:06.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"eventStatusCodes":["open","upcoming"],"..."}
2024-03-22 04:55:06.0000	health:DescribeEventAggregates	AWS Internal	{"filter":{"startTimes":[{"from":"Mar 15, 2024 4:55:0..."}

8

IAM_Users

eventNameFull	requestParameters
---------------	-------------------

18

CLI vs Console



IAM_Users

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:55:29.0000	iam:ListUsers	AWS Internal	{"maxItems":1000}
2024-03-22 04:55:30.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}
2024-03-22 04:55:30.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}
2024-03-22 04:55:30.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}
2024-03-22 04:55:32.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}
2024-03-22 04:55:32.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}
2024-03-22 04:55:32.0000	iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}
2024-03-22 04:55:32.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}
2024-03-22 04:55:32.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}
2024-03-22 04:55:32.0000	iam:ListMFADevices	aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}
2024-03-22 04:55:33.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}
2024-03-22 04:55:33.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}
2024-03-22 04:55:33.0000	iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}
2024-03-22 04:55:34.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}
2024-03-22 04:55:34.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Daniel_Bohannon"}
2024-03-22 04:55:34.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"No_Permissions"}
2024-03-22 04:55:35.0000	iam:GetAccessKey	aws-internal/3 aws-sdk-java/...	{"keyId":"AKIAPERSHENDETJEMIQ1"}
2024-03-22 04:55:35.0000	iam:GetAccessKey	aws-internal/3 aws-sdk-java/...	{"keyId":"AKIAPERSHENDETJEMIQ2"}

18

13

1

8

CLI vs Console



IAM_Users_CreateUser_Step1

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:55:46.0000	ssso:DescribeRegisteredRegions	AWS Internal	
2024-03-22 04:55:46.0000	organizations:ListDelegatedAdministrators	AWS Internal	
2024-03-22 04:55:46.0000	organizations:DescribeOrganization	AWS Internal	
2024-03-22 04:55:46.0000	iam:GetAccountPasswordPolicy	AWS Internal	

4

18

13

1

8

IAM_Users_CreateUser_Step1B (attach policy)

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:56:23.0000	iam:ListPolicies	AWS Internal	{"maxItems":1000,"onlyAttached":false}
2024-03-22 04:56:23.0000	iam:ListGroup	AWS Internal	{"maxItems":1000}
2024-03-22 04:56:23.0000	iam:GetGroup	aws-internal/3 aws-sdk-java/...	{"groupName":"customGroup1"}
2024-03-22 04:56:23.0000	iam:GetGroup	aws-internal/3 aws-sdk-java/...	{"groupName":"customGroup2"}
2024-03-22 04:56:24.0000	iam:ListPolicies	AWS Internal	{"maxItems":1000,"marker":"AFB1SALqql7Kp/vCLGK..."}
2024-03-22 04:56:24.0000	iam:ListAttachedGroupPolicies	aws-internal/3 aws-sdk-java/...	{"groupName":"customGroup1"}
2024-03-22 04:56:24.0000	iam:ListAttachedGroupPolicies	aws-internal/3 aws-sdk-java/...	{"groupName":"customGroup2"}
2024-03-22 04:56:25.0000	iam:ListPolicies	aws-internal/3 aws-sdk-java/...	{"scope":"AWS","onlyAttached":false,"pathPrefix":"/"}
2024-03-22 04:56:25.0000	iam:ListPolicies	aws-internal/3 aws-sdk-java/...	{"scope":"AWS","onlyAttached":false,"pathPrefix":"/"}
2024-03-22 04:56:25.0000	iam:ListPolicies	aws-internal/3 aws-sdk-java/...	aws:iam::200802171337:policy/Per...
2024-03-22 04:56:25.0000	iam:ListPolicies	aws-internal/3 aws-sdk-java/...	aws:iam::200802171337:policy/Per...
2024-03-22 04:56:25.0000	iam:ListPolicies	aws-internal/3 aws-sdk-java/...	aws:iam::200802171337:policy/Per...

15

CLI vs Console



IAM_Users_CreateUser_Step1B (attach policy)

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:56:23.0000	iam:ListPolicies	AWS Internal	{"maxItems":1000,"onlyAttached":false}
2024-03-22 04:56:23.0000	iam:ListGroup	AWS Internal	{"maxItems":1000}
2024-03-22 04:56:23.0000	iam:GetGroup	aws-internal/3 aws-sdk-java/...	{"groupName":"customGroup1"}
2024-03-22 04:56:23.0000	iam:GetGroup	aws-internal/3 aws-sdk-java/...	{"groupName":"customGroup2"}
2024-03-22 04:56:24.0000	iam:ListPolicies	AWS Internal	{"maxItems":1000,"marker":"AFB1SALqql7Kp/vCLGK..."}
2024-03-22 04:56:24.0000	iam:ListAttachedGroupPolicies	aws-internal/3 aws-sdk-java/...	{"groupName":"customGroup1"}
2024-03-22 04:56:24.0000	iam:ListAttachedGroupPolicies	aws-internal/3 aws-sdk-java/...	{"groupName":"customGroup2"}
2024-03-22 04:56:25.0000	iam:ListPolicies	aws-internal/3 aws-sdk-java/...	{"scope":"AWS","onlyAttached":false,"pathPrefix":"/"}
2024-03-22 04:56:26.0000	iam:ListPolicies	aws-internal/3 aws-sdk-java/...	{"scope":"AWS","onlyAttached":false,"pathPrefix":"/"}
2024-03-22 04:56:26.0000	iam:GetPolicy	aws-internal/3 aws-sdk-java/...	{"policyArn":"arn:aws:iam::200802171337:policy/Per..."}
2024-03-22 04:56:26.0000	iam:GetPolicy	aws-internal/3 aws-sdk-java/...	{"policyArn":"arn:aws:iam::200802171337:policy/Per..."}
2024-03-22 04:56:26.0000	iam:GetPolicy	aws-internal/3 aws-sdk-java/...	{"policyArn":"arn:aws:iam::200802171337:policy/per..."}
2024-03-22 04:56:27.0000	iam:GetPolicy	aws-internal/3 aws-sdk-java/...	{"policyArn":"arn:aws:iam::200802171337:policy/Per..."}
2024-03-22 04:56:27.0000	iam:GetPolicy	aws-internal/3 aws-sdk-java/...	{"policyArn":"arn:aws:iam::200802171337:policy/Per..."}
2024-03-22 04:56:27.0000	iam:GetPolicy	aws-internal/3 aws-sdk-java/...	{"policyArn":"arn:aws:iam::200802171337:policy/per..."}

15

18

13

4

1

8

Cre

CLI vs Console



IAM_Users_CreateUser_Step2

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:57:34.0000	iam:ListUsers	AWS Internal	{"maxItems":1000}
2024-03-22 04:57:35.0000	iam:CreateUser	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:35.0000	iam:AttachUserPolicy	AWS Internal	{"userName":"krileva","policyArn":"arn:aws:iam::aws:..."}

3

18

13

4

1

IAM_Users_SPECIFICUSER_Permissions

eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:57:59.0000	iam:ListUserTags	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:ListUserPolicies	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:ListMFADevices	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:ListGroupsForUser	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:ListAttachedUserPolicies	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:ListAccessKeys	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:GetUser	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:GetLoginProfile	awscli/2.11.17 (Linux; x86_64; Java/11.0.16)	{"userName":"krileva"}
2024-03-22 04:58:00.0000	iam:ListAccessKeys	awscli/2.11.17 (Linux; x86_64; Java/11.0.16)	{"userName":"krileva"}
	access-analyzer:ListAccessAnalyzerPolicies	awscli/2.11.17 (Linux; x86_64; Java/11.0.16)	{"arn":"arn:aws:iam::200802171337:user/kri..."}

10

15

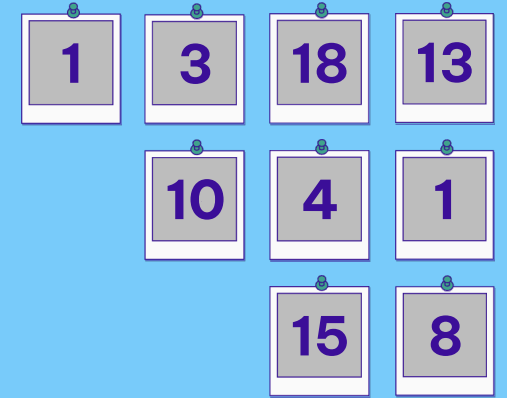
8

CLI vs Console



IAM_Users_SPECIFICUSER_CreateAccessKey

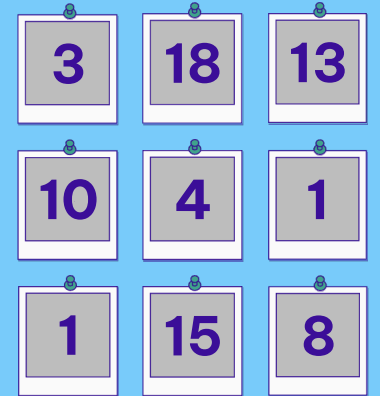
eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:58:57.0000	iam:CreateAccessKey	AWS Internal	{"userName":"krileva"}



CLI vs Console



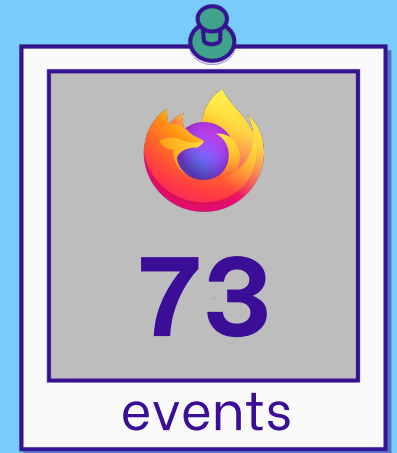
eventCount	userAgent
28	AWS Internal
2	aws-internal/3 aws-sdk-java/1.12.676 Linux/5.10.210-178.852.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/17.0.10+9-LTS java/1.8.0_402 vendor/N/A cfg/retry-mode/standard
25	aws-internal/3 aws-sdk-java/1.12.679 Linux/5.10.210-178.852.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/17.0.10+9-LTS java/1.8.0_402 vendor/N/A cfg/retry-mode/standard
5	aws-internal/3 aws-sdk-java/1.12.679 Linux/5.10.210-178.855.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/17.0.10+9-LTS java/1.8.0_402 vendor/N/A cfg/retry-mode/standard
3	health.amazonaws.com
10	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0



CLI vs Console

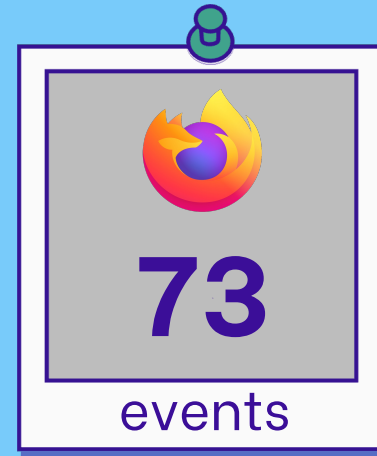
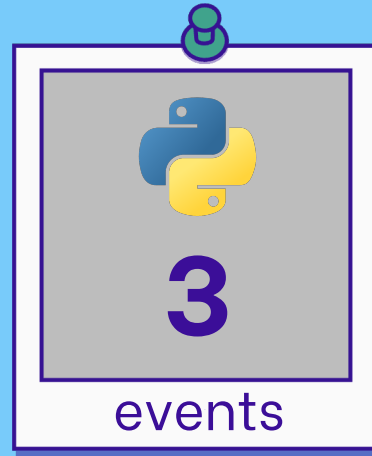
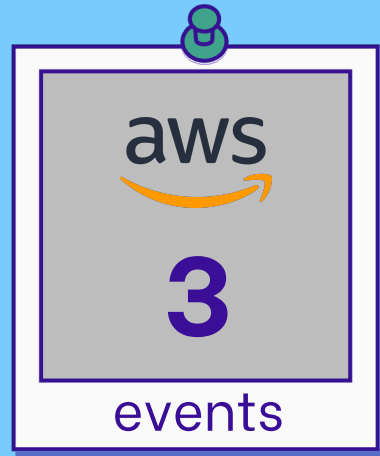


eventCount	userAgent
28	AWS Internal
2	aws-internal/3 aws-sdk-java/1.12.676 Linux/5.10.210-178.852 amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/17.0.10+9-LTS java/1.8.0_402 vendor/N/A cfg/retry-mode/standard
25	aws-internal/3 aws-sdk-java/1.12.679 Linux/5.10.210-178.852 amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/17.0.10+9-LTS java/1.8.0_402 vendor/N/A cfg/retry-mode/standard
5	aws-internal/3 aws-sdk-java/1.12.679 Linux/5.10.210-178.855 amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/17.0.10+9-LTS java/1.8.0_402 vendor/N/A cfg/retry-mode/standard
3	health.amazonaws.com
10	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0



73
events

CLI vs Console



Worst Case Scenarios



IAM_Users

eventNameFull	userAgent	requestParameters
iam:ListUsers	AWS Internal	{"maxItems":1000}
iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"} {"userName":"Daniel_Bohannon"} {"userName":"No_Permissions"}
iam:ListSigningCertificates	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"} {"userName":"Daniel_Bohannon"} {"userName":"No_Permissions"}
iam:ListMFADevices	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"} {"userName":"Daniel_Bohannon"} {"userName":"No_Permissions"}
iam:ListGroupsForUser	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"} {"userName":"Daniel_Bohannon"} {"userName":"No_Permissions"}
iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"} {"userName":"Daniel_Bohannon"} {"userName":"No_Permissions"}
iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}

$n=3$

```

{"userName":"Andi_Ahmeti"}
{"userName":"Daniel_Bohannon"}
{"userName":"No_Permissions"}
    
```

1

+

5n

+

$[0, 2n]$

1

+

$5(3) = 15$

+

$[0, 2(3)] = 2$

18

Worst Case Scenarios



$$1 + 5n + [0, 2n]$$



IAM_Users

n=20

- Page size
- 20 rows
 - 50 rows
 - 100 rows

eventNameFull	eventCount	dcount_usersOrKeys	usersOrKeys
iam:ListUsers	1	0	[]
iam:GetLoginProfile	20	20	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListSigningCertificates	20	20	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListMFADevices	20	20	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListGroupsForUser	20	20	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListAccessKeys	20	20	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:GetAccessKeyLastUsed	40	40	["AKIAPERSHENDETJEMIQ1","AKIAPERSHENDETJEMIQ2",...]

$$1 + 5(20) + [0, 2(20)] =$$

141

n=50

- Page size
- 20 rows
 - 50 rows
 - 100 rows

eventNameFull	eventCount	dcount_usersOrKeys	usersOrKeys
iam:ListUsers	1	0	[]
iam:GetLoginProfile	50	50	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListSigningCertificates	50	50	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListMFADevices	50	50	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListGroupsForUser	50	50	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListAccessKeys	50	50	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:GetAccessKeyLastUsed	100	100	["AKIAPERSHENDETJEMIQ1","AKIAPERSHENDETJEMIQ2",...]

$$1 + 5(50) + [0, 2(50)] =$$

351

n=100

- Page size
- 20 rows
 - 50 rows
 - 100 rows

eventNameFull	eventCount	dcount_usersOrKeys	usersOrKeys
iam:ListUsers	1	0	[]
iam:GetLoginProfile	100	100	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListSigningCertificates	100	100	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListMFADevices	100	100	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListGroupsForUser	100	100	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:ListAccessKeys	100	100	["Bagel","Bear_Claw","Beignet","Churro","Cinnamon_Roll",...]
iam:GetAccessKeyLastUsed	200	200	["AKIAPERSHENDETJEMIQ1","AKIAPERSHENDETJEMIQ2",...]

$$1 + 5(100) + [0, 2(100)] =$$

701

Worst Case Scenarios



$$1 + 5n + [0, 2n]$$



$$21 + 4n$$

n=100

S3_Buckets

Page size
● 100 buckets

eventNameFull	eventCount	dcount_buckets	buckets
s3:ListBuckets	2	0	[]
s3:GetStorageLensConfiguration	1	0	[]
s3:GetStorageLensConfiguration	1	0	[]
s3:GetStorageLensDashboardDataInternal	2	0	[]
ec2:DescribeRegions	1	0	[]
health:DescribeEventAggregates	2	0	[]
notifications:ListNotificationHubs	1	0	[]
s3:GetAccountPublicAccessBlock	11	0	[]
s3:ListAccessPoints	100	100	["bureki","doner","gjevrek","golden_eagle",...]
s3:GetBucketPolicyStatus	100	100	["bureki","doner","gjevrek","golden_eagle",...]
s3:GetBucketPublicAccessBlock	100	100	["bureki","doner","gjevrek","golden_eagle",...]
s3:GetBucketAcl	100	100	["bureki","doner","gjevrek","golden_eagle",...]

$$21 + 4(100) = 421$$

In Summary...

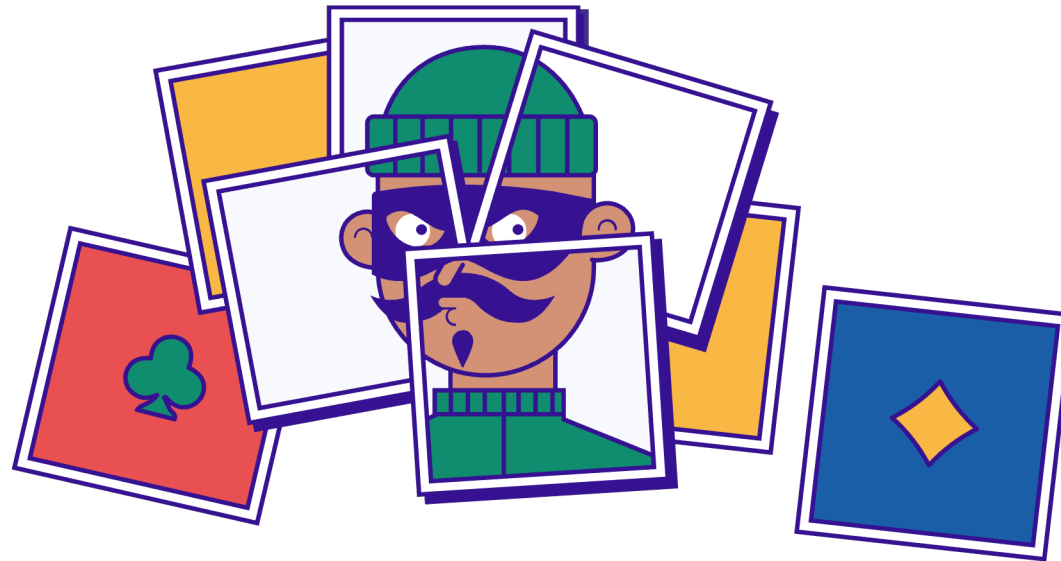


#Aggregation

In Summary...

IAM_Users_CreateUser

IAM_Users

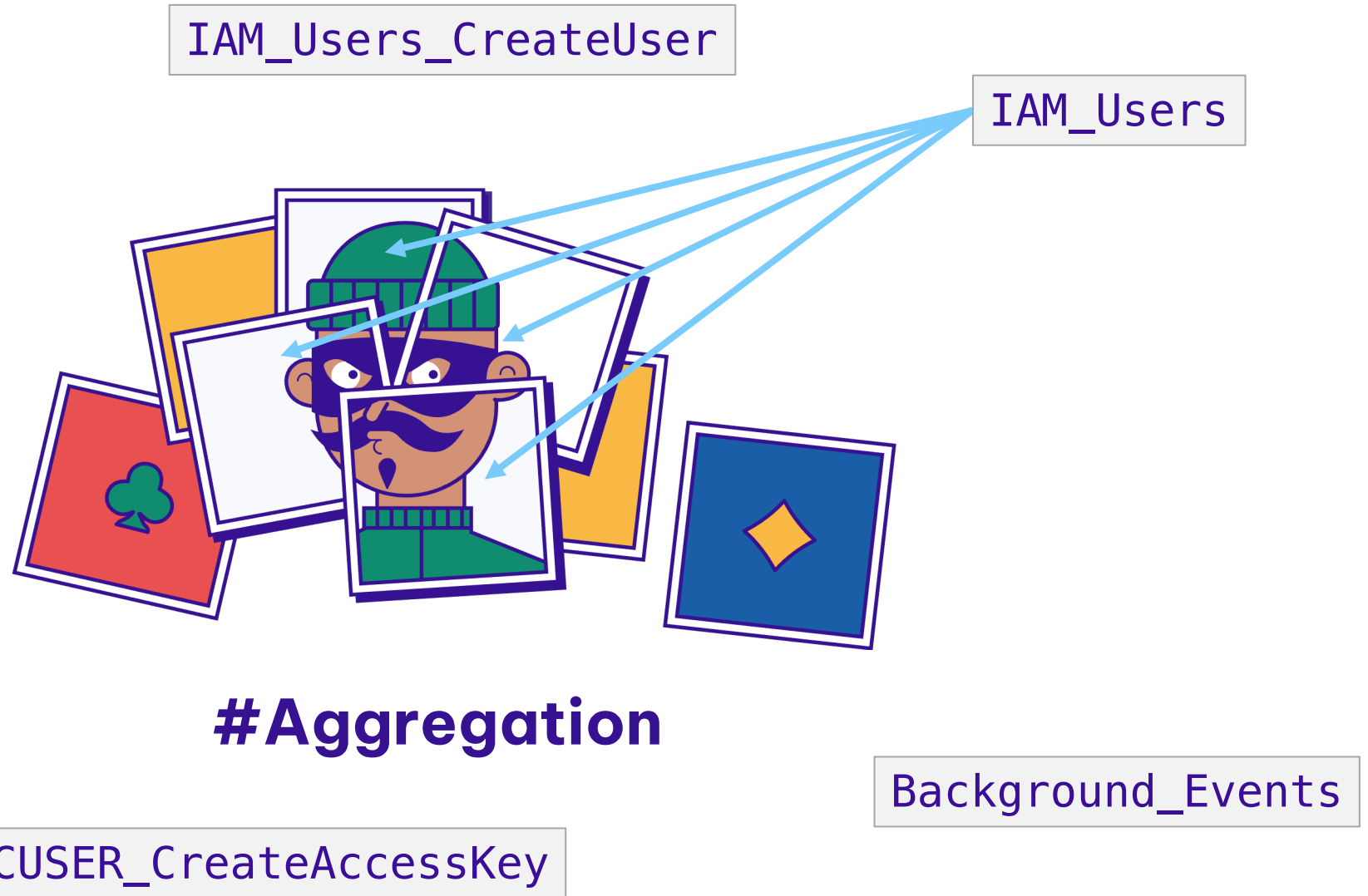


#Aggregation

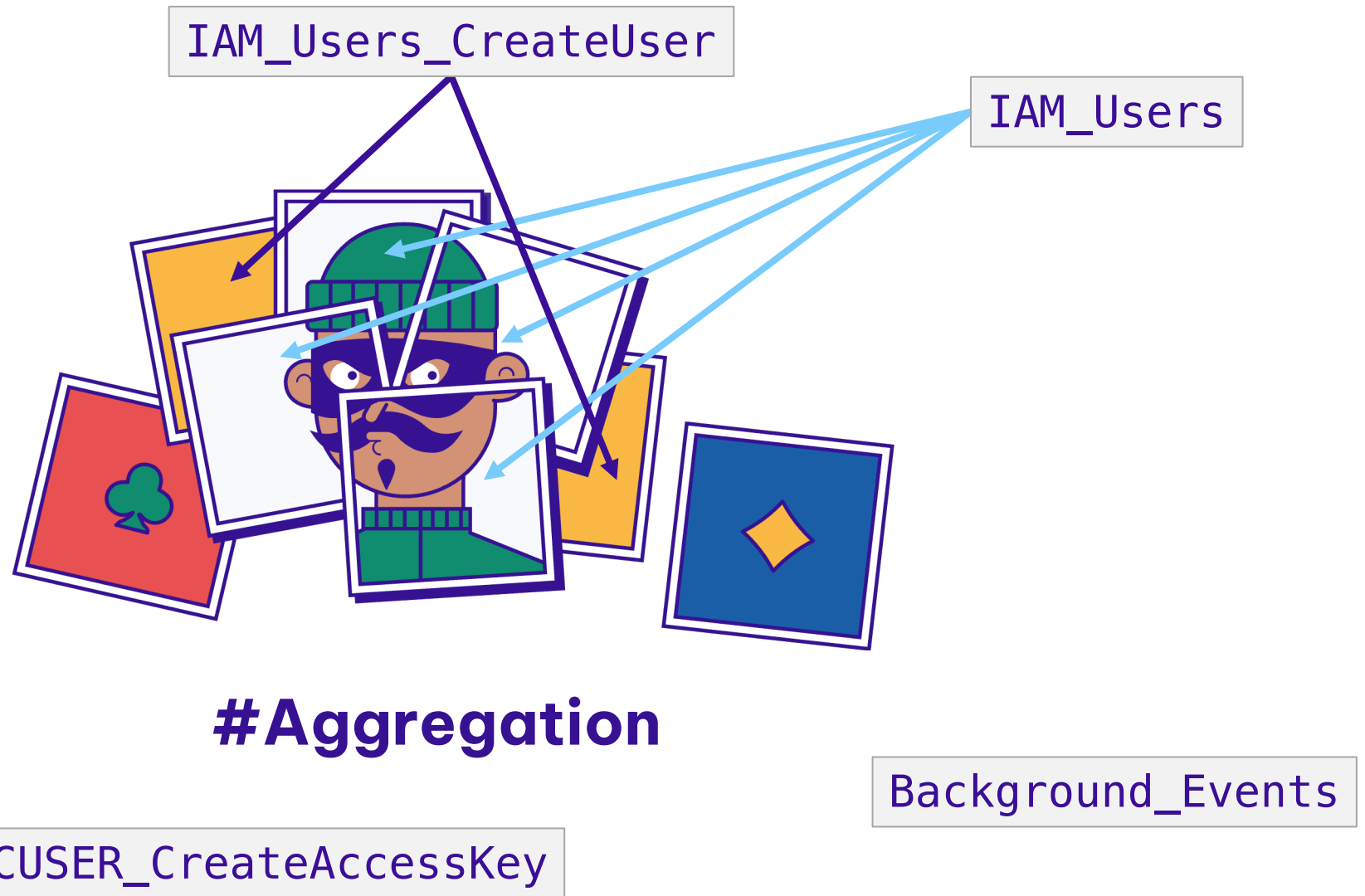
Background_Events

IAM_Users_SPECIFICUSER_CreateAccessKey

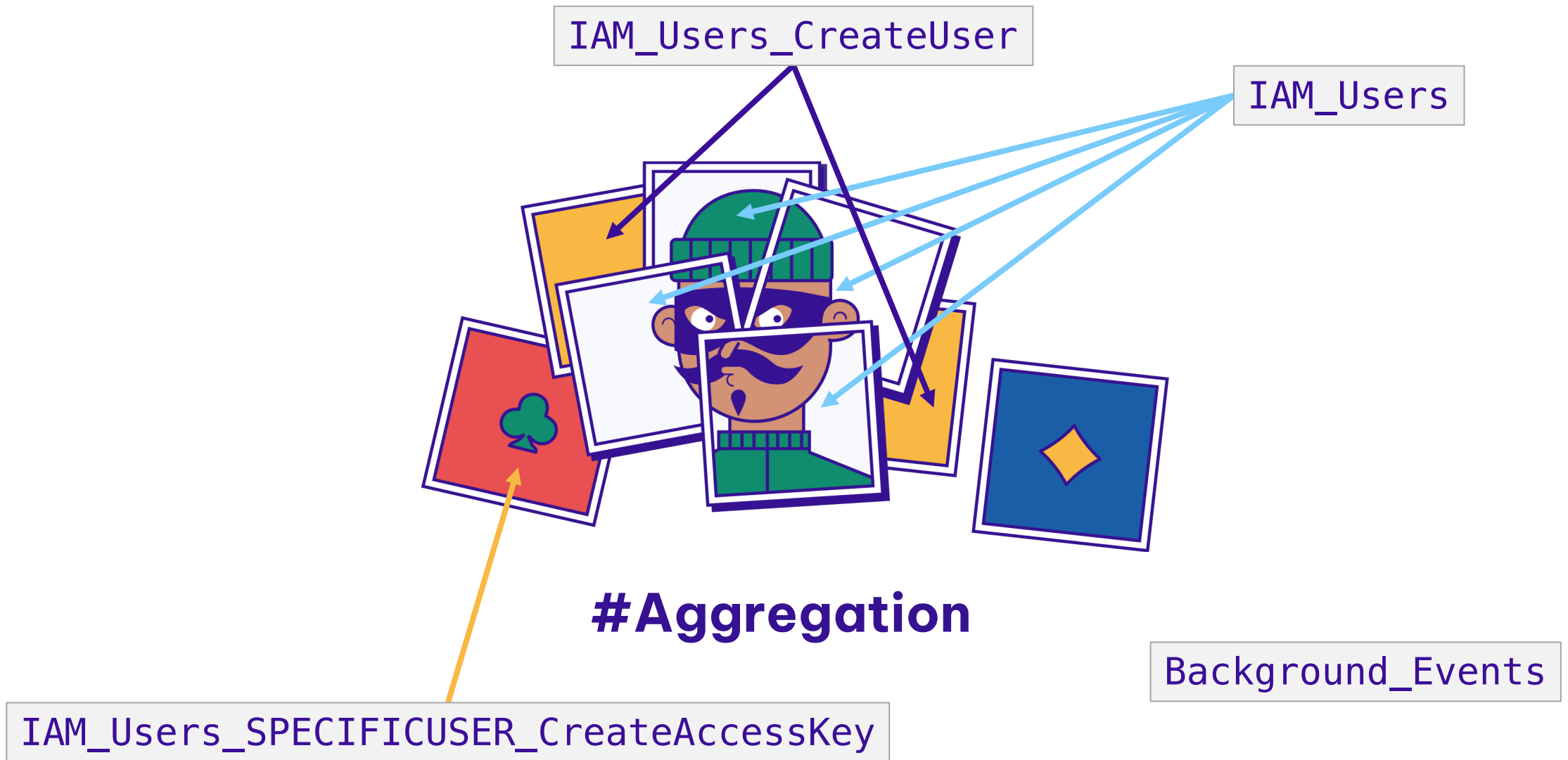
In Summary...



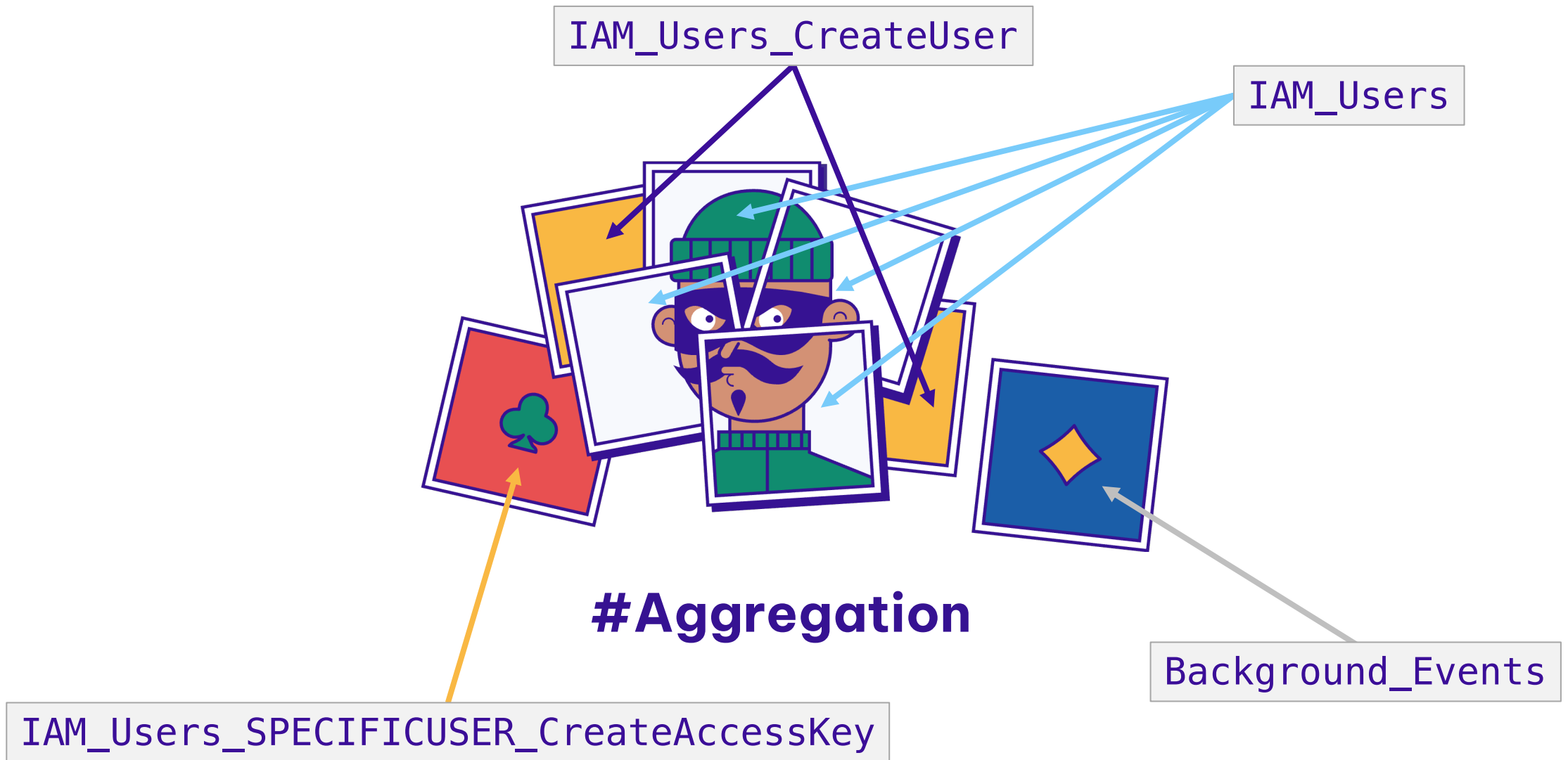
In Summary...



In Summary...

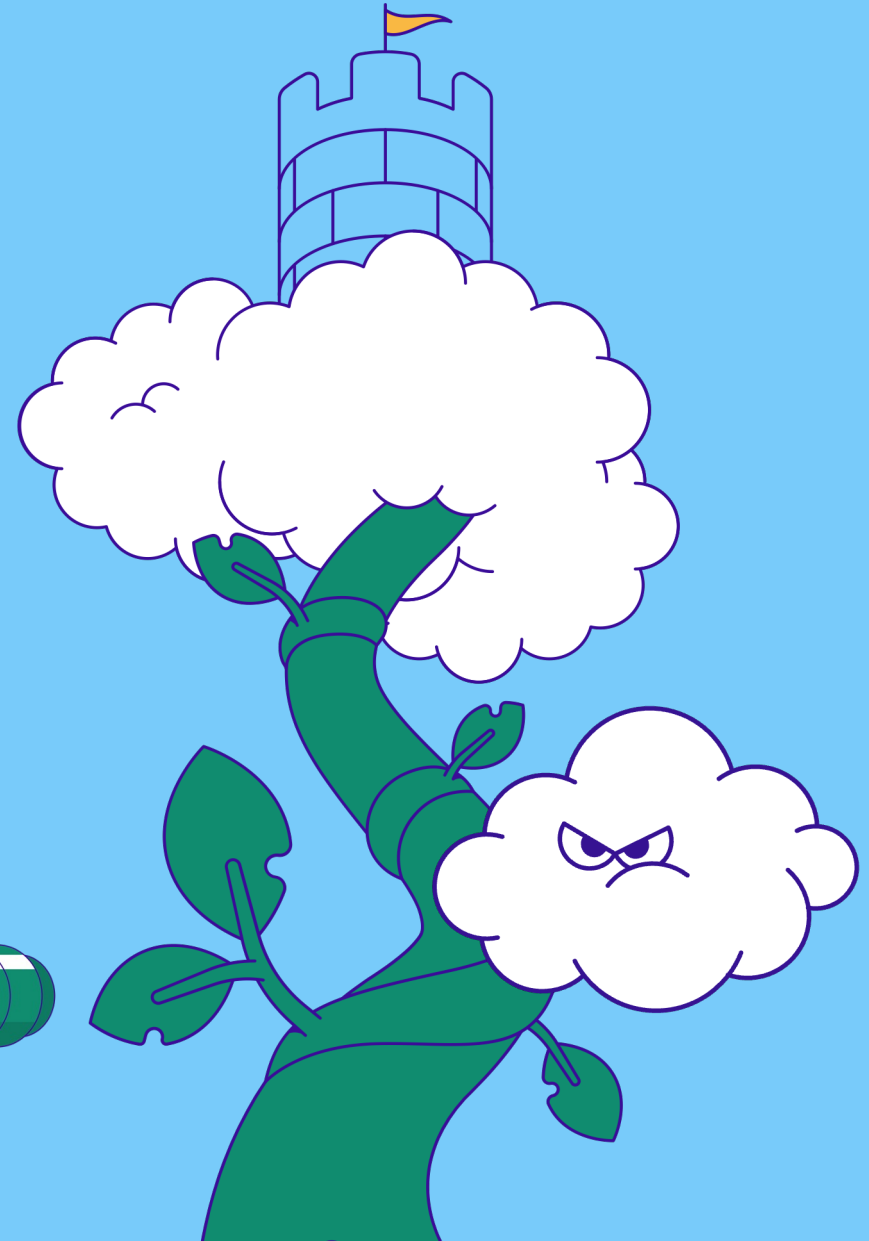
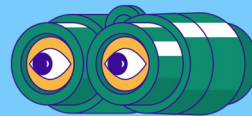


In Summary...

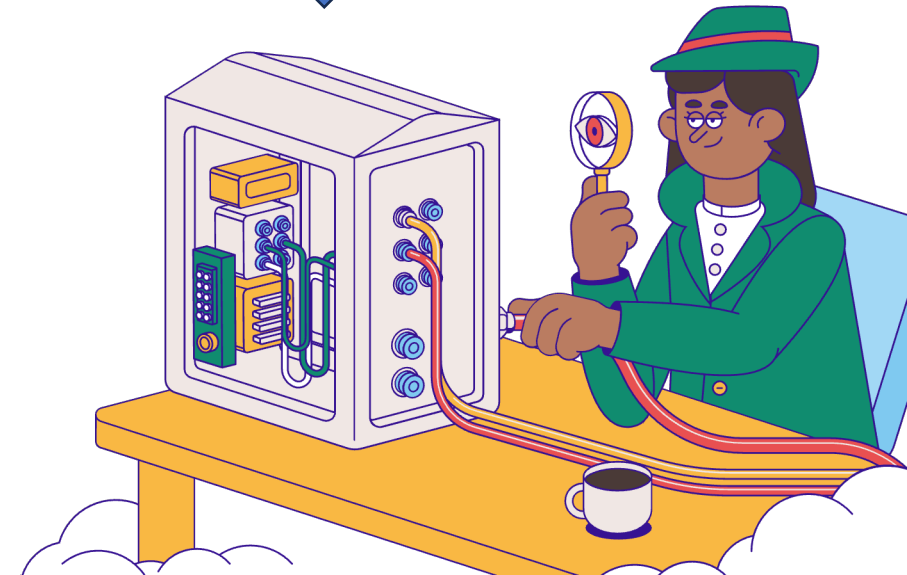
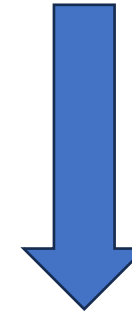
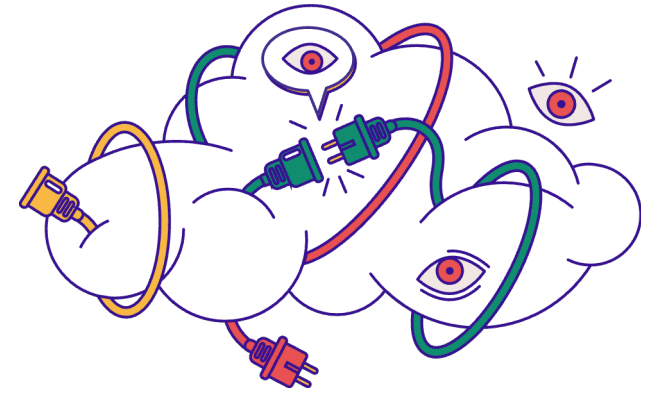
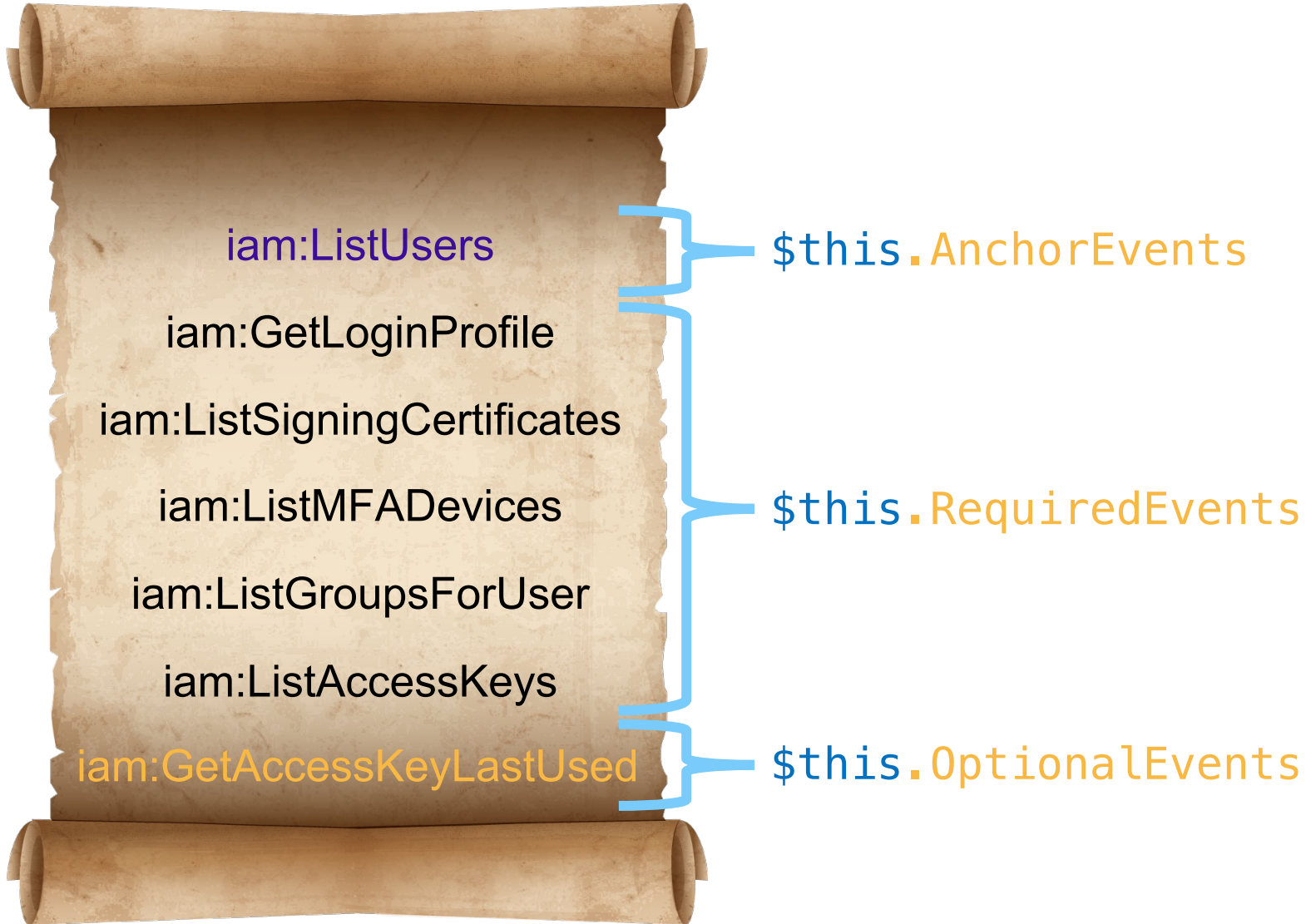


AGENDA

- Introduction
- Cloud Logs for Defenders
- **PROBLEM:** Noisy Console Logs
- **SOLUTION:** Mapping for Clarity
- Tool Demo + Release



2-Pass Approach – Labels + Signals



Signal Definition

```
( [LabelType]::IAM_Users) {  
  $this.Service = 'IAM'  
  $this.Name = 'Clicked IAM->Users'  
  $this.Summary = 'Clicked IAM->Users which displays all IAM Users in paged format.'  
  $this.Url = 'https://{{awsRegion}}.console.aws.amazon.com/iamv2/home?region={{awsRegion}}#/users'  
  $this.AnchorEvents = @( 'iam:ListUsers' )  
  $this.RequiredEvents = @(  
    'iam:GetLoginProfile',  
    'iam:ListAccessKeys',  
    'iam:ListGroupsForUser',  
    'iam:ListMFADevices',  
    'iam:ListSigningCertificates',  
    'iam:ListUsers'  
  )  
  # iam:GetAccessKeyLastUsed only executed if 1+ IAM Users with 1+ Access Keys are defined.  
  $this.OptionalEvents = @( 'iam:GetAccessKeyLastUsed' )  
  # Current mapping scenario generates events over longer-than-normal timespan, so increasing  
  # default lookback/lookahead values when aggregating nearby events surrounding AnchorEvents.  
  $this.LookbackInSeconds = 5  
  $this.LookaheadInSeconds = 35  
}
```



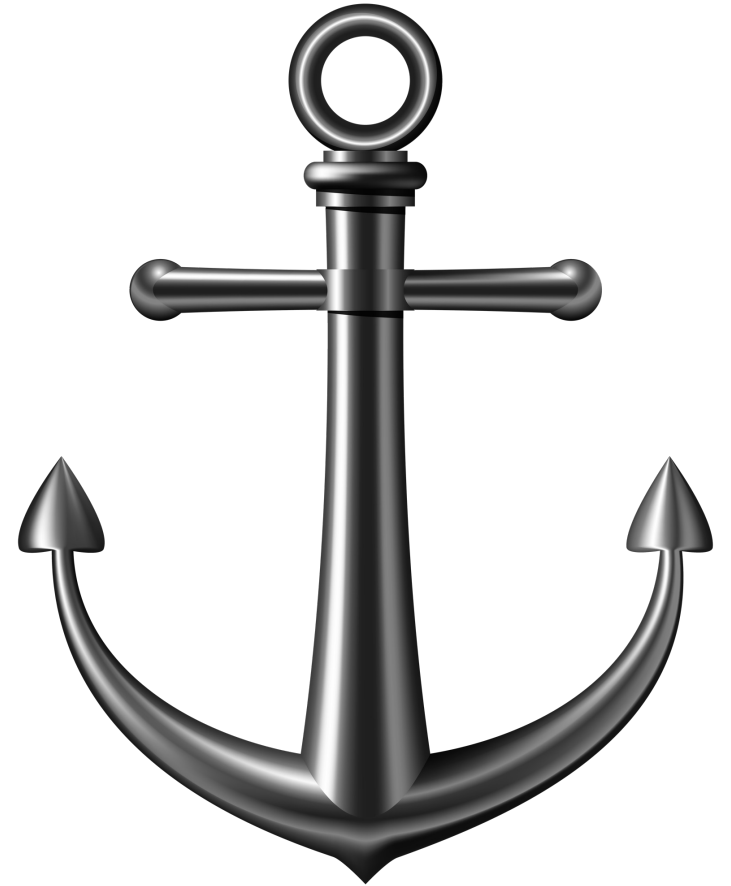
Pass #1 - Label Assignment (Per-Event)

```
'ListUsers' {  
  # E.g. {"maxItems":1000}  
  if (  
    $requestParametersStr -ceq '{"maxItems":1000}' -and `  
    $userAgentFamily -eq [UserAgentFamily]::AWS_Internal  
  )  
  {  
    [LabelType]::IAM_BrowserRefresh  
    [LabelType]::IAM  
    [LabelType]::IAM_Users_CreateUser_Step2  
    [LabelType]::IAM_Users  
    [LabelType]::IAM_UserGroups  
    [LabelType]::IAM_Users_CreateUser  
  }  
}
```



Pass #2 – Signal Evaluation (Grouped Events)

- Iterate over all events w/Labels
- Stop at each Anchor event
- Test each Label for current Anchor event:
 - Gather nearby unmapped events with same Label
 - If gathered events match current Label's Signal definition -> create Signal object
 - Else try next Label




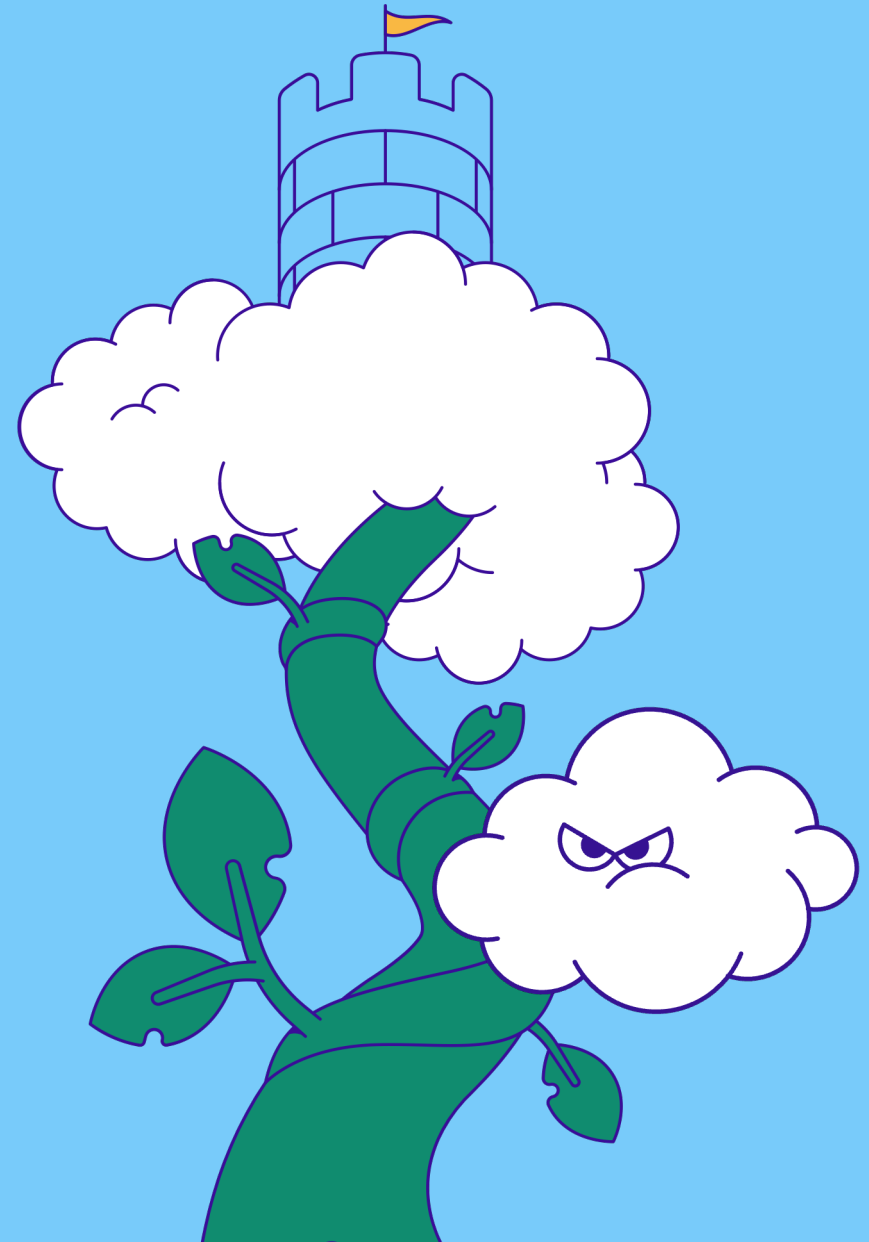
Add'l Cool Tricks & Capabilities

- Modification of Signal names, summaries & URLs based on data extracted from all related events
- Each Signal contains dictionary of extracted data
- Signal lookback scenarios for:
 - Modifying previous Signals
 - Changing Label for current Signal
 - Merging previous Signals
 - Extracting data from previous Signals to be used in current Signal

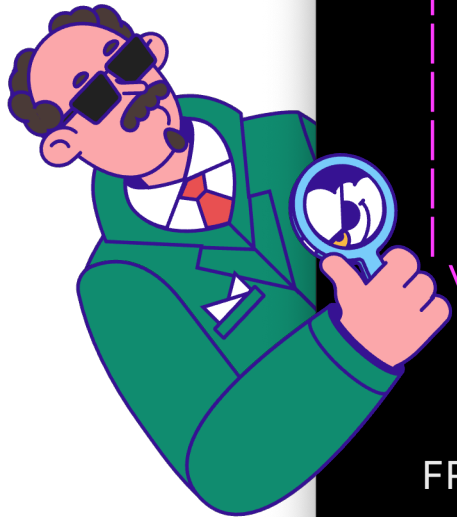
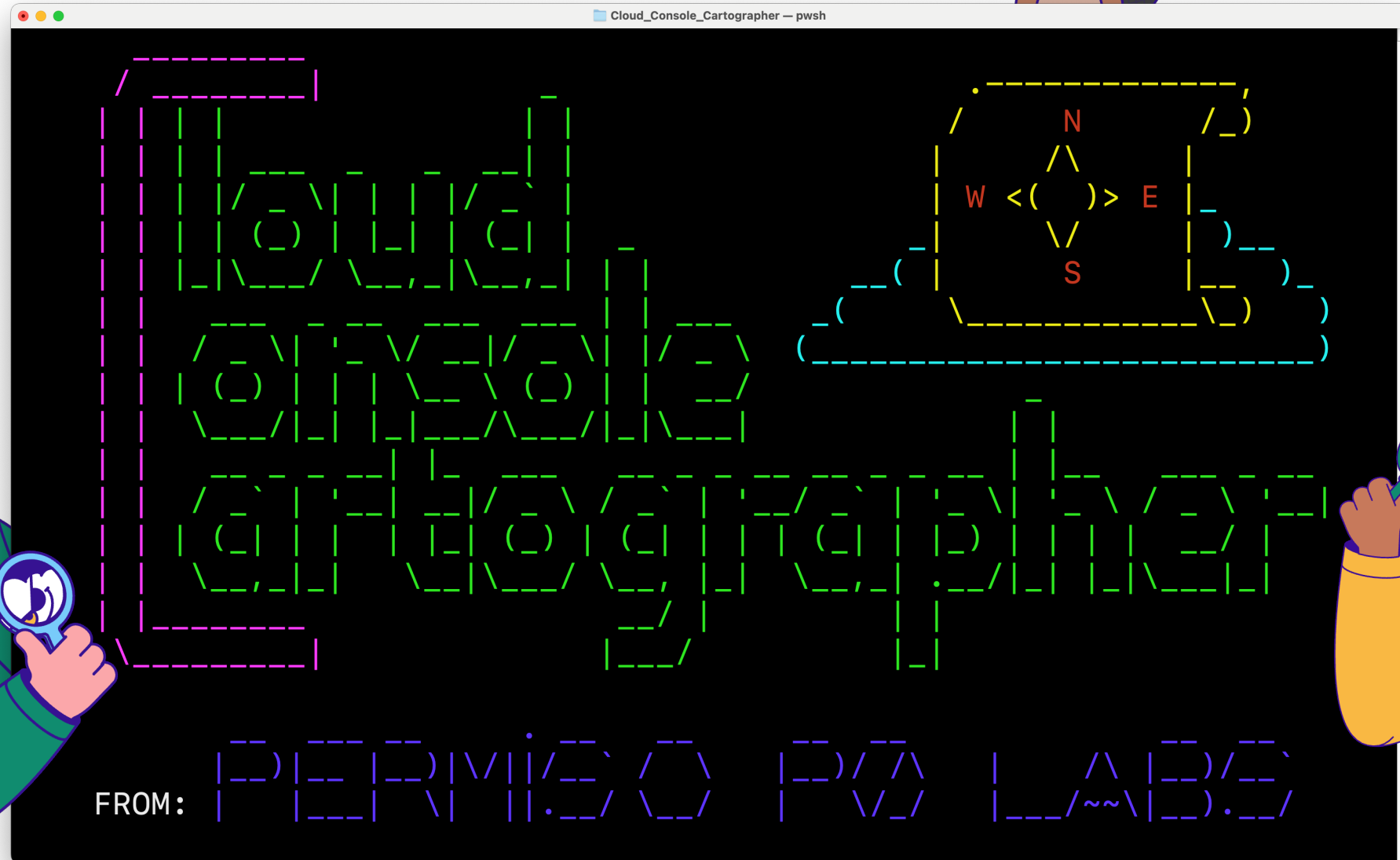


AGENDA

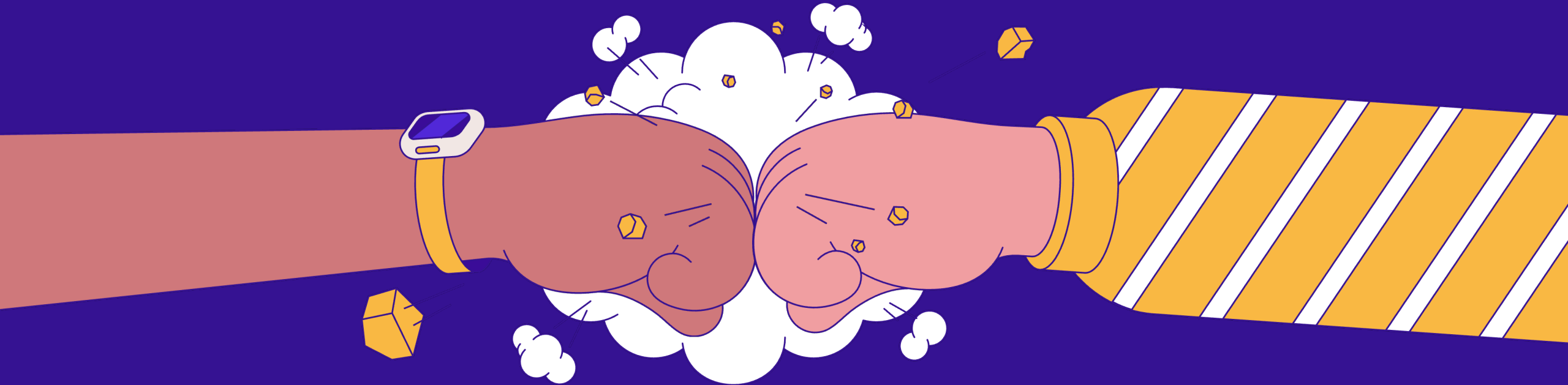
- Introduction
- Cloud Logs for Defenders
- **PROBLEM:** Noisy Console Logs
- **SOLUTION:** Mapping for Clarity
- Tool Demo + Release 

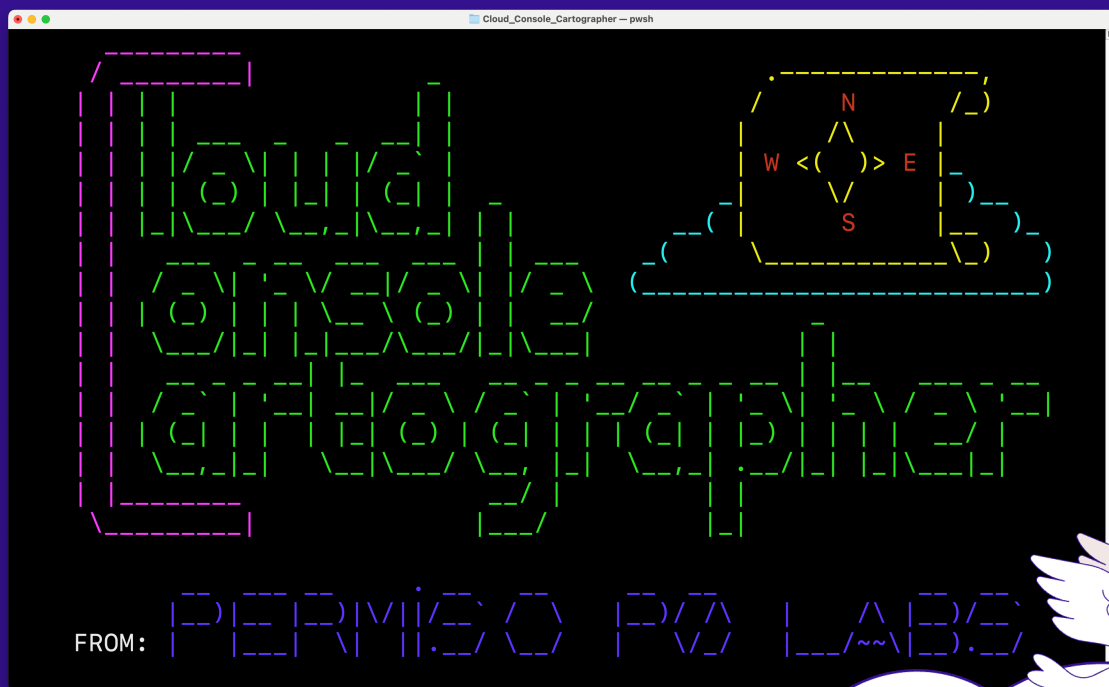
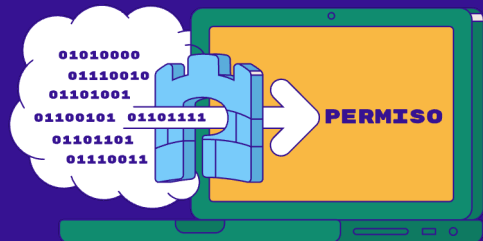


DEMO + Public Tool Release



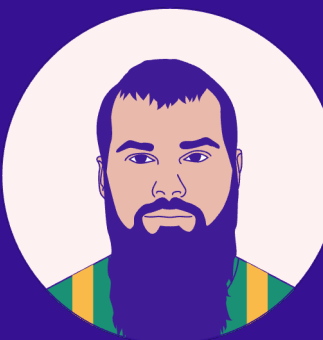
THANKS FOR YOUR TIME!





**ANDI
AHMETI**

andi-ahmeti



**DANIEL
BOHANNON**

danielhbohannon

@SecEagleAnd1



@danielhbohannon



<https://github.com/Permiso-io-tools/CloudConsoleCartographer>