

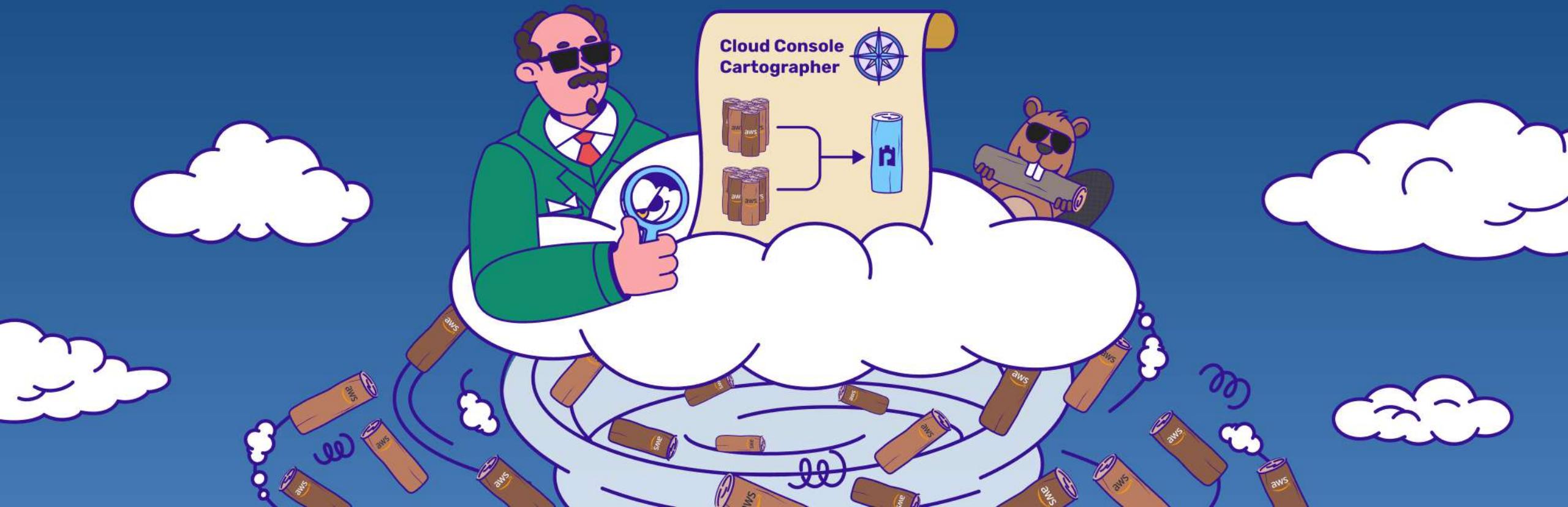


PERMISO

black hat
ASIA 2024

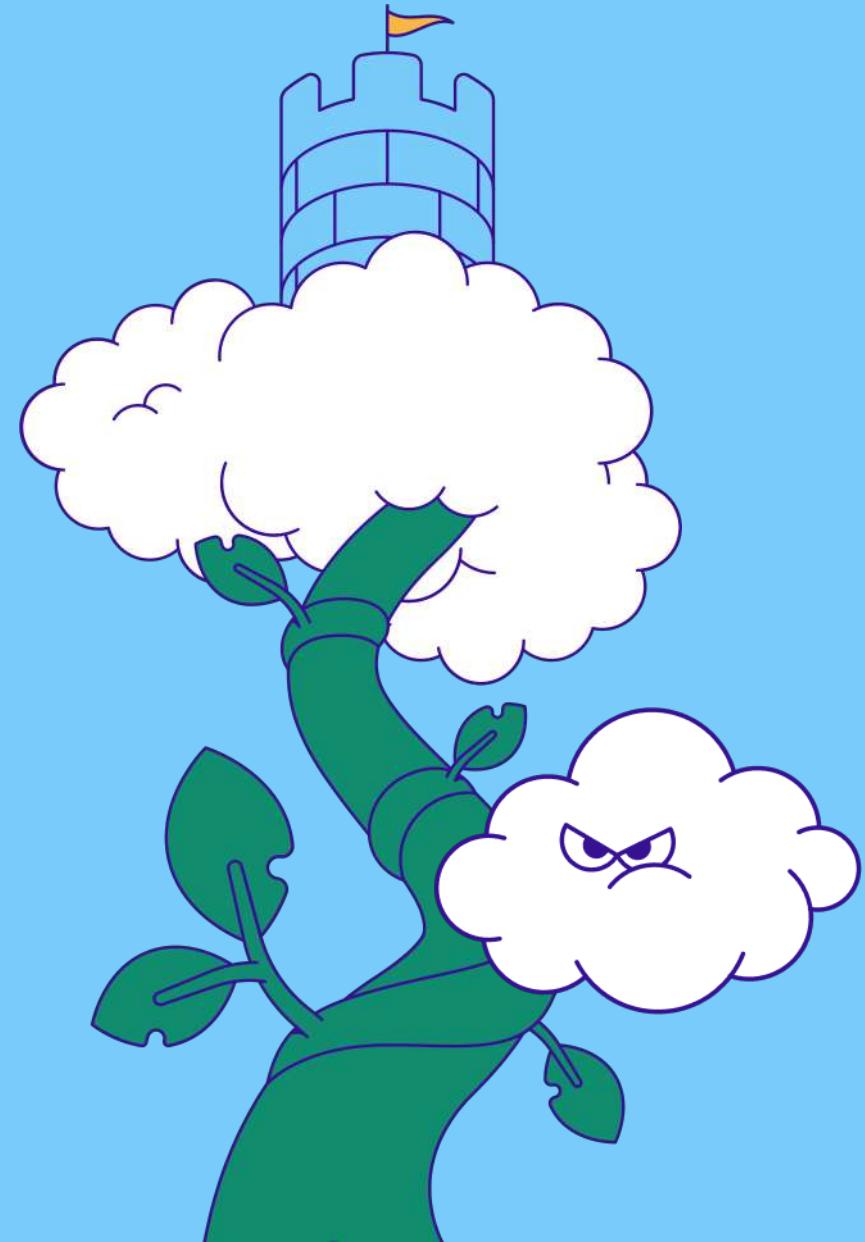
Cloud Console Cartographer

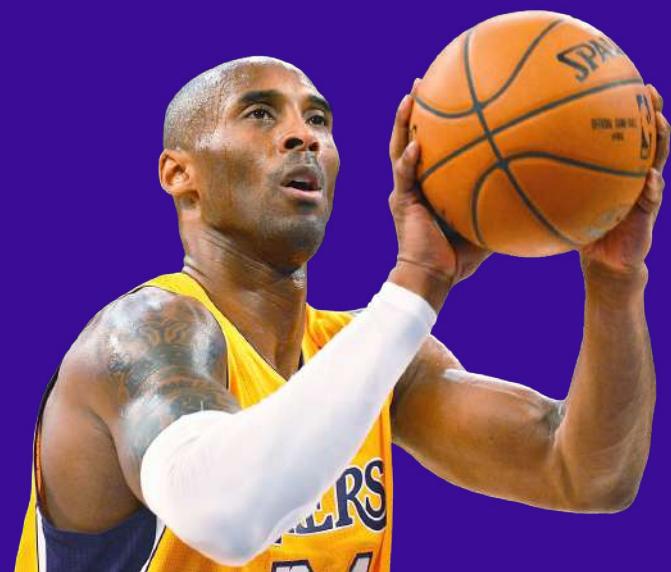
Tapping Into Mapping > Slogging Thru Logging



AGENDA

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





ANDI AHMETI
ASSOCIATE THREAT RESEARCHER



Kosovo



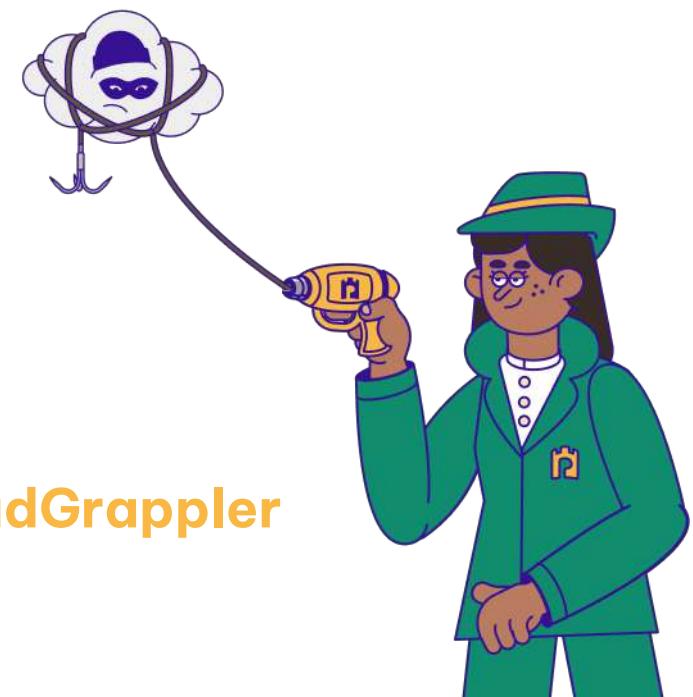
@SecEagleAnd1



andi-ahmeti



Permisio-io-tools/**CloudGrappler**





DANIEL BOHANNON
PRINCIPAL THREAT RESEARCHER



USA

MANDIANT (5 yrs)

 **Microsoft** (2 yrs)



@daniel**h**bohannon



daniel**h**bohannon

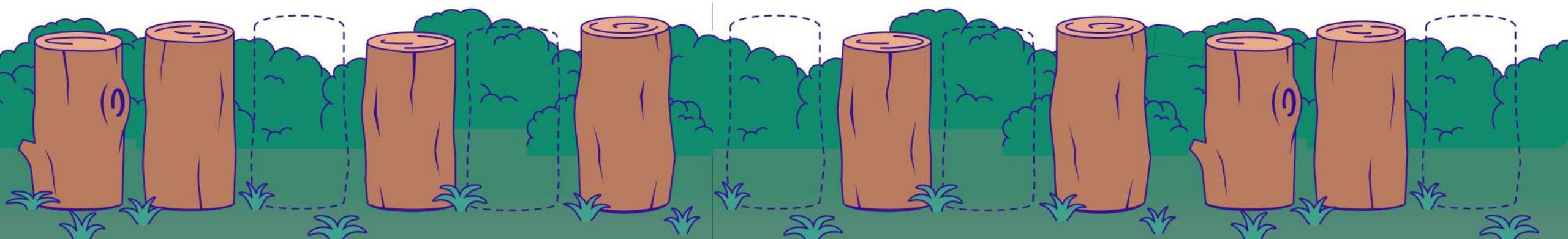
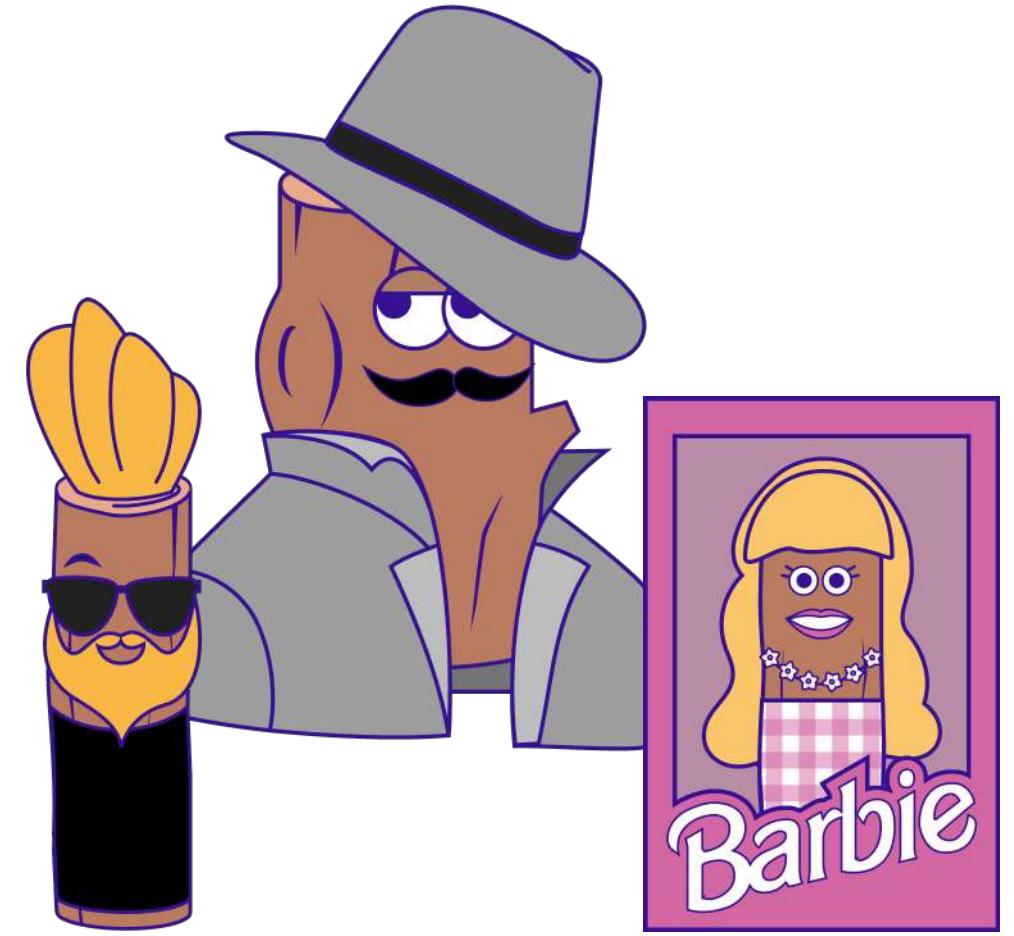


danielbohannon/**Invoke-Obfuscation**
/Invoke-CradleCrafter
/Invoke-DOSfuscation
/Revoke-Obfuscation



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



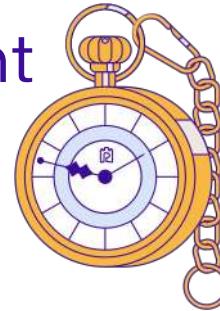
On-Prem vs Cloud Logs (*Data source, not storage location*)

- 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 “**fingerprints**” in user/attacker activity



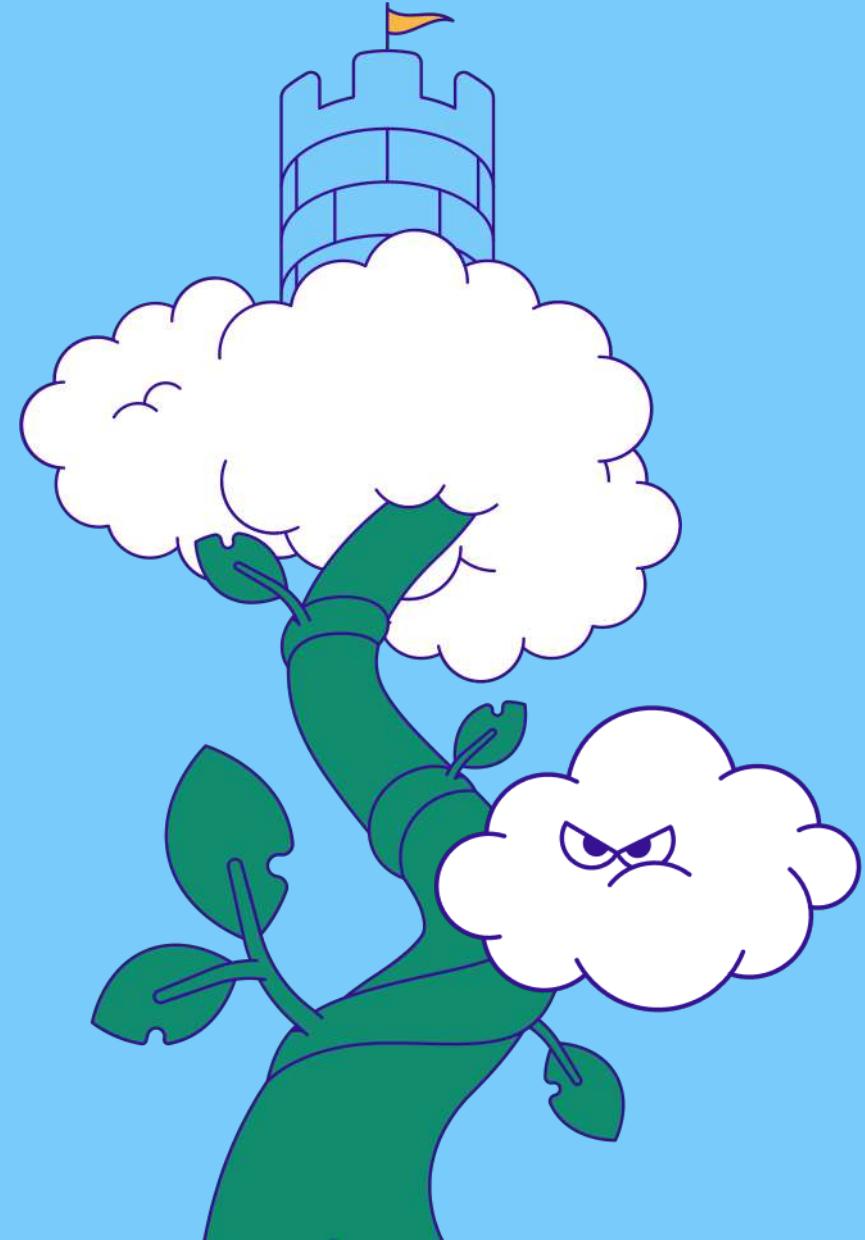
On-Prem vs Cloud Logs (*Data source, not storage location*)

- 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": "2024-04-01T13:33:37.000000Z",  
  "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": "AIDA12345678ABCDEFGH",  
      "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 Event history page. The left sidebar includes options like Dashboard, Event history (selected), Insights, Lake (Dashboard, Query, Event data stores, Integrations), Trails, and Settings. The main content area displays the 'Event history (1) Info' section, which says 'Event history shows you the last 90 days of management events.' Below this is a 'Lookup attributes' section with dropdowns for 'Event name' set to 'CreateUser' and a date range from '2024-04-01T13:00:00-04:00' to '2024-04-01T14:00:00-04:00'. A table below lists one event: 'CreateUser' from 'iam.amazonaws.com' with resource type 'AWS::IAM::User' and resource name 'arn:aws:iam::200802171337:user/krileva, AI'. At the bottom, it says '0 / 5 events selected'.

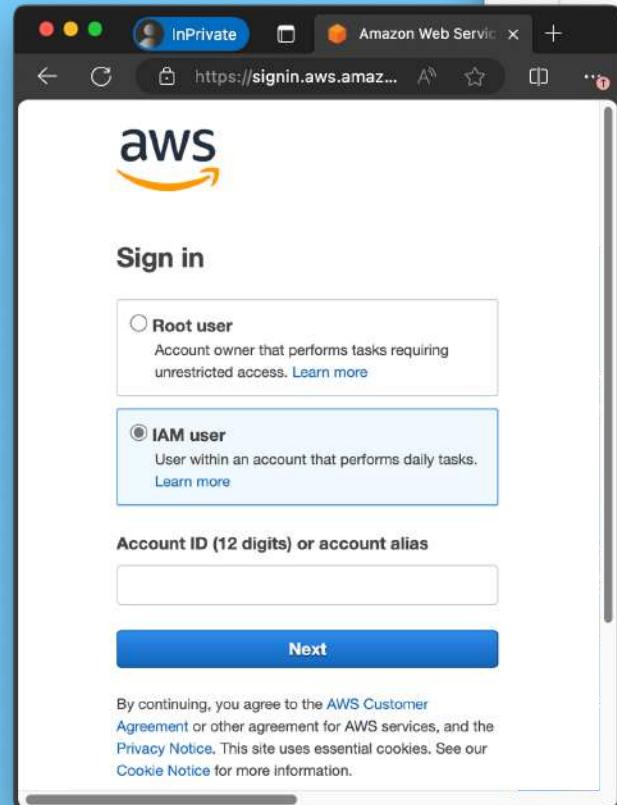
```
bash-3.2$ bash-3.2$ aws cloudtrail lookup-events \
>   --lookup-attributes AttributeKey=EventName,AttributeValue/CreateUser \
>   --start-time 2024-04-01T013:00:00 --end-time 2024-04-01T14:00:00
{
  "Events": [
    {
      "EventId": "db014773-abcd-1234-5678-133337c0ffee",
      "EventName": "CreateUser",
      "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": "AIDA12345678ABCDEFGH"
        },
        {
          "ResourceType": "AWS::IAM::User",
          "ResourceName": "krileva"
        }
      ],
      "CloudTrailEvent": "{\"eventVersion\":\"1.09\",\"userIdentity\":{\"type\":\"IAMUser\",\"principalId\":\"AIDA12345678ABCDEFGH\",\"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\":\"AIDA12345678ABCDEFGH\",\"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\"}"
    }
  ]
}
bash-3.2$
```

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

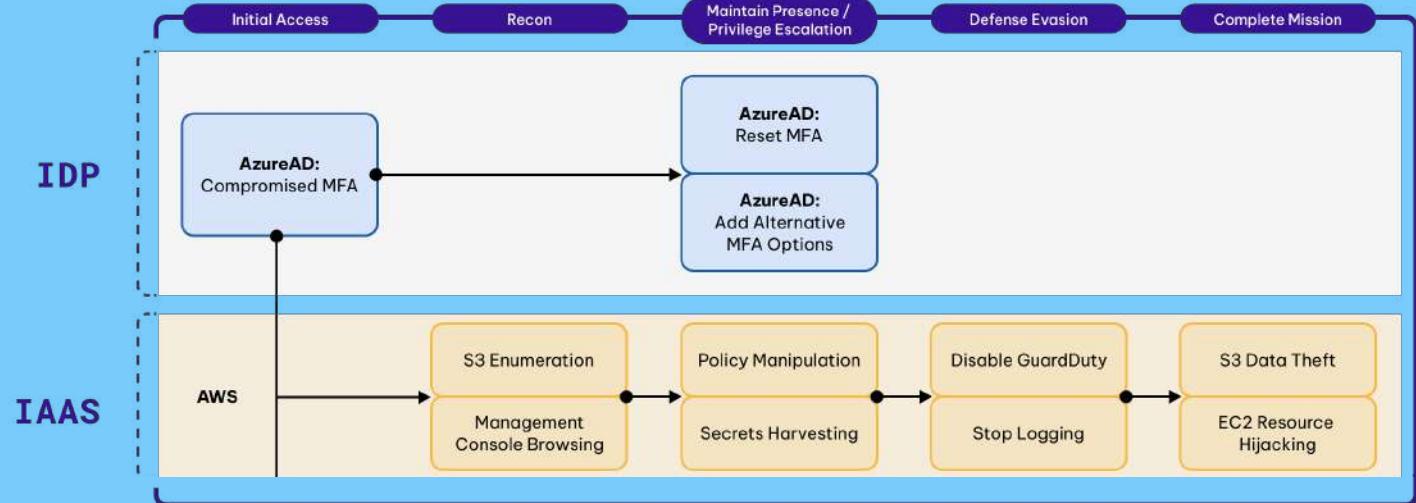
A screenshot of the AWS Management Console Getting Started Guide. The title is 'What is the AWS Management Console?'. Below the title is a 'PDF' link. A text block defines the AWS Management Console as 'a web application that comprises and refers to a broad collection of service consoles for managing AWS resources.' This text is highlighted with a yellow box. Another paragraph explains that when you first sign in, you see the console home page, which 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. At the bottom, there is a code snippet in a white box:

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

A screenshot of the Microsoft Azure sign-in page. It has a blue header with the Microsoft logo and 'Sign in' text. Below the header is a 'Sign in' input field with placeholder text 'Email, phone, or Skype'. Underneath the input field are links for 'No account? Create one!' and 'Can't access your account?'. At the bottom right is a 'Next' button. On the left side, there are icons for social logins: GitHub, Facebook, and LinkedIn.

Console Usage in the Wild

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

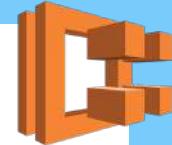


Console Usage in the Wild

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

Permissions

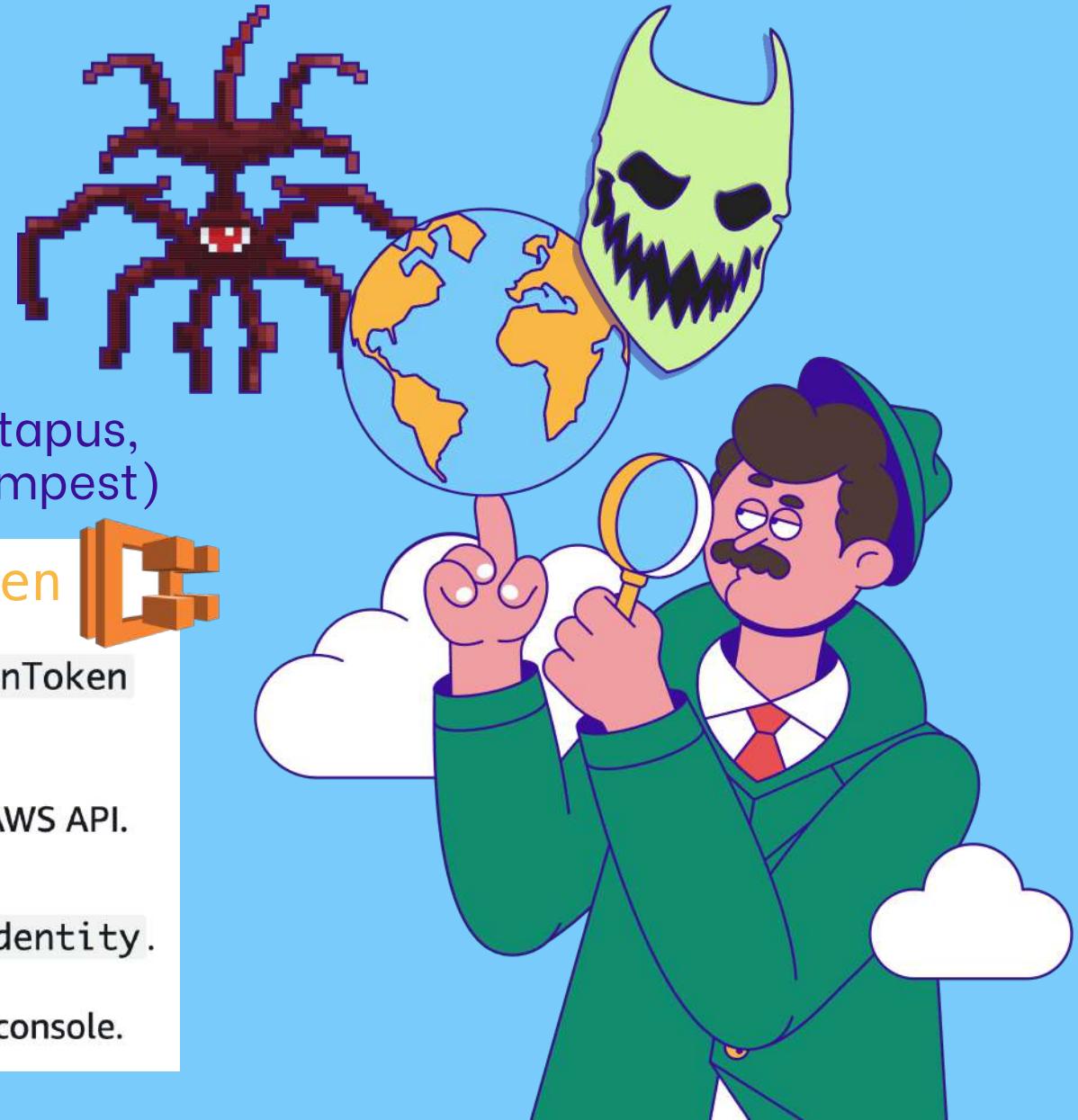
sts:GetFederationToken



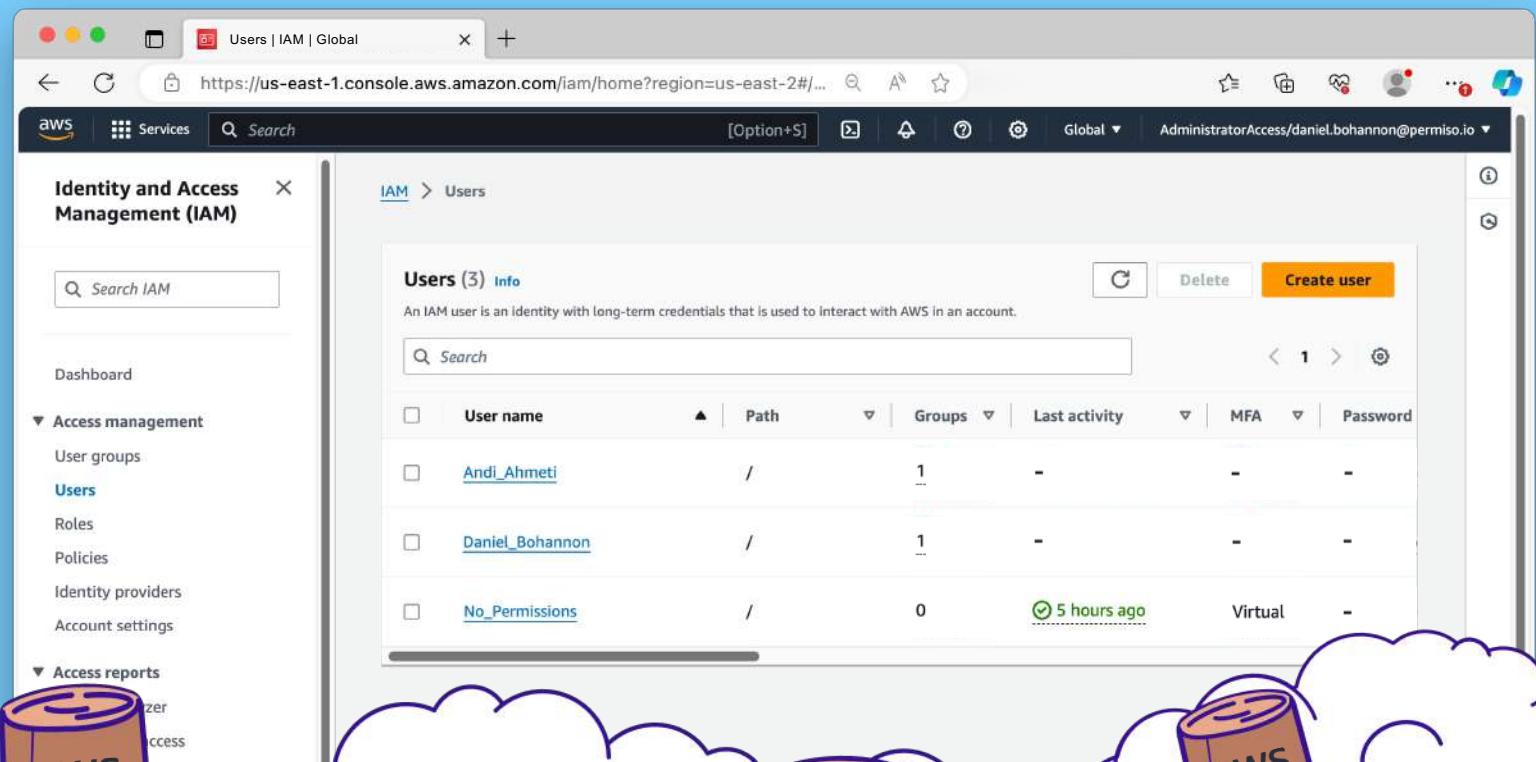
You can use the temporary credentials created by `GetFederationToken` in any AWS service with the following exceptions:

- 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.

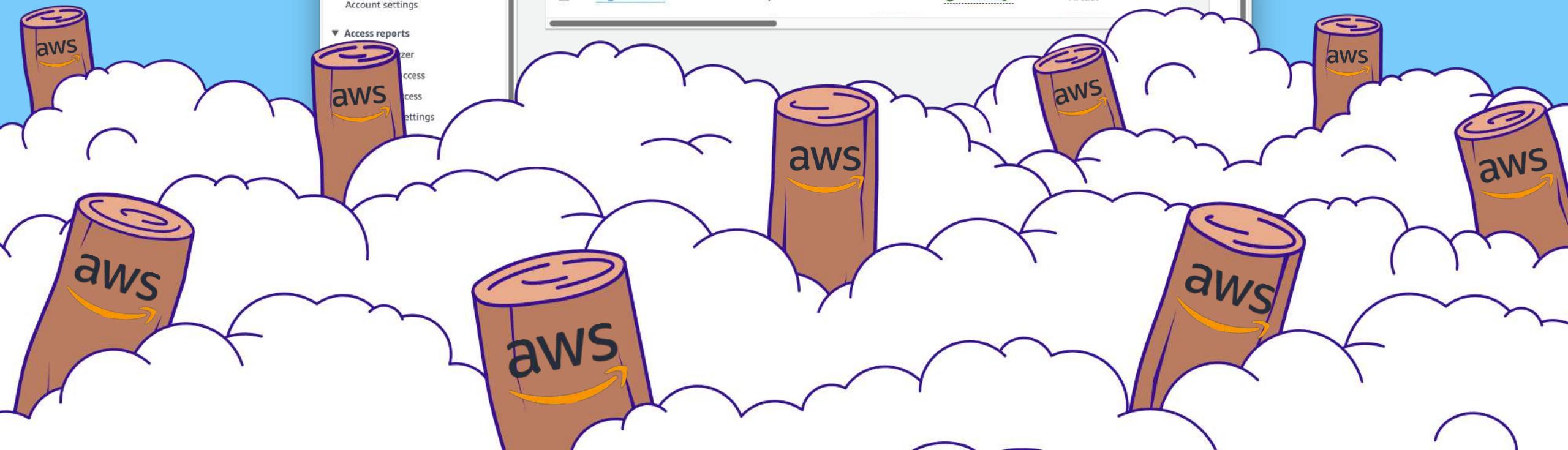


Log

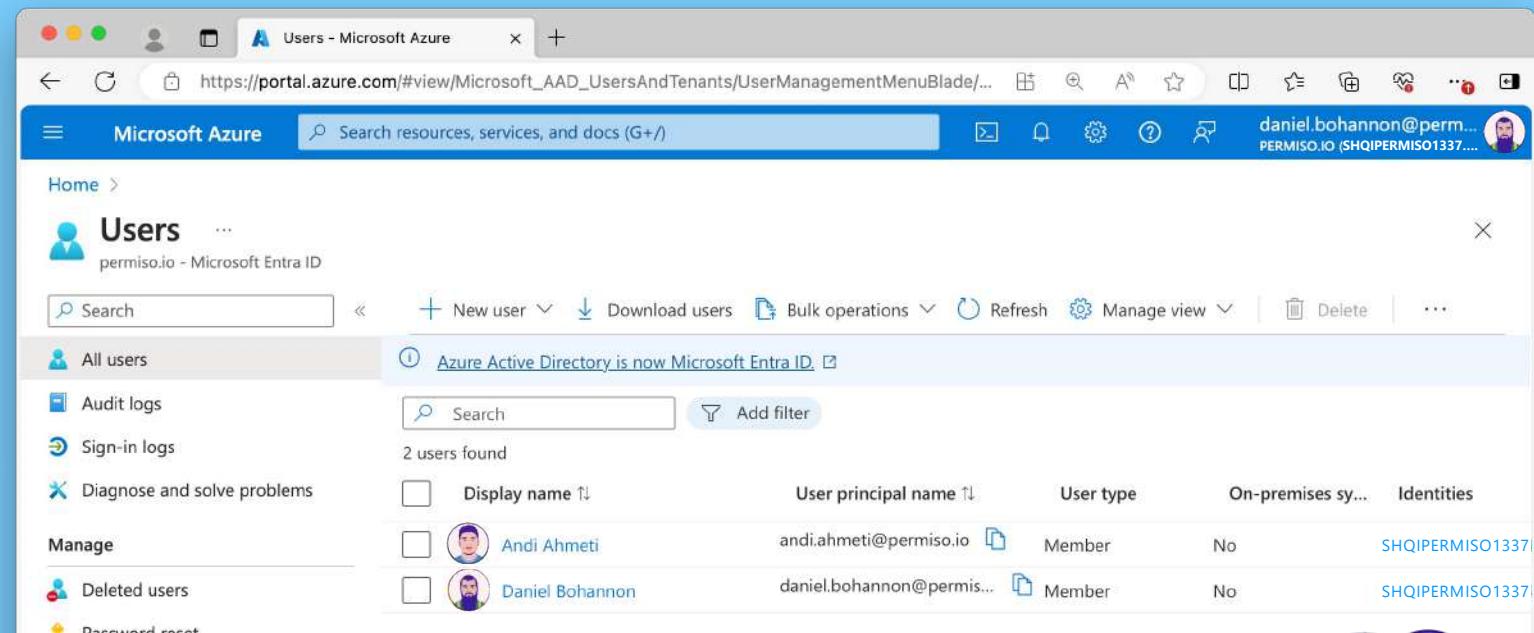


The screenshot shows the AWS Identity and Access Management (IAM) service in a web browser. The URL is <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/>. The browser window has a title bar "Users | IAM | Global" and a tab "Users | IAM | Global". The main content area is titled "Identity and Access Management (IAM)" and "Users (3) Info". A table lists three users:

User name	Path	Groups	Last activity	MFA	Password
Andi_Ahmeti	/	1	-	-	-
Daniel_Bohannon	/	1	-	-	-
No_Permissions	/	0	5 hours ago	-	Virtual



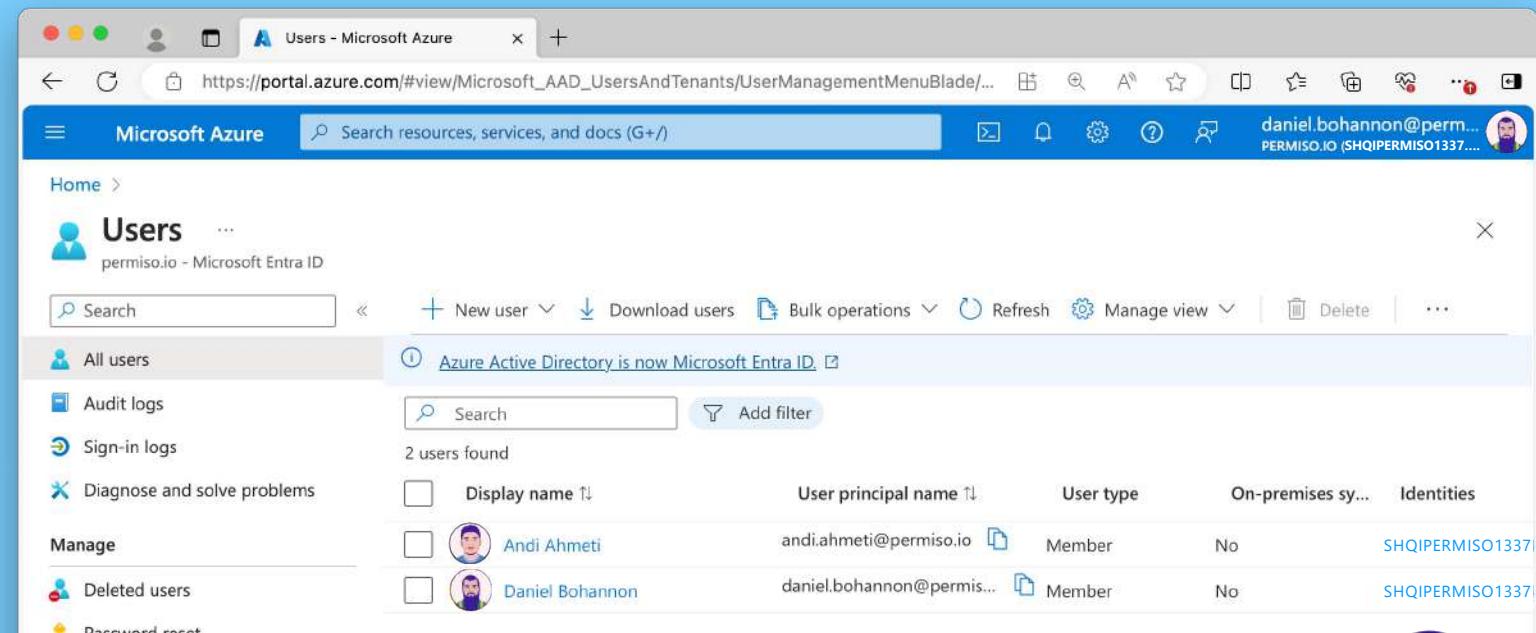
Log



The screenshot shows the Microsoft Azure portal's User Management interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and a user profile for "daniel.bohannon@permiso.io". The main content area is titled "Users" and shows a list of users under the "permiso.io - Microsoft Entra ID" tenant. A sidebar on the left provides links for "Audit logs", "Sign-in logs", "Diagnose and solve problems", "Manage", "Deleted users", "Password reset", and "User settings". A banner at the top of the main area states "Azure Active Directory is now Microsoft Entra ID". The user list table has columns for "Display name", "User principal name", "User type", "On-premises sync status", and "Identities". Two users are listed: Andi Ahmeti (display name: Andi Ahmeti, user principal name: andi.ahmeti@permiso.io, user type: Member, on-premises sync: No, identities: SHQIPERMISO1337) and Daniel Bohannon (display name: Daniel Bohannon, user principal name: daniel.bohannon@permiso.io, user type: Member, on-premises sync: No, identities: SHQIPERMISO1337).

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

Log



The screenshot shows the Microsoft Azure portal's User Management interface. The left sidebar lists options like Audit logs, Sign-in logs, Diagnose and solve problems, Manage (Deleted users, Password reset, User settings, Bulk operation results), and Troubleshooting + Support (New support request). The main area displays a table of users:

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

A banner at the top right of the main area says "Azure Active Directory is now Microsoft Entra ID".



Users - Microsoft Azure

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

daniel.bohannon@permiso.io (SHQIPERMISO1337...)

Home > Users

All users

Azure Active Directory is now Microsoft Entra ID.

Search Add filter

2 users found

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

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Deleted users

Password reset

User settings

Bulk operation results

Troubleshooting + Support

New support request



NO, N-NOT YOU.

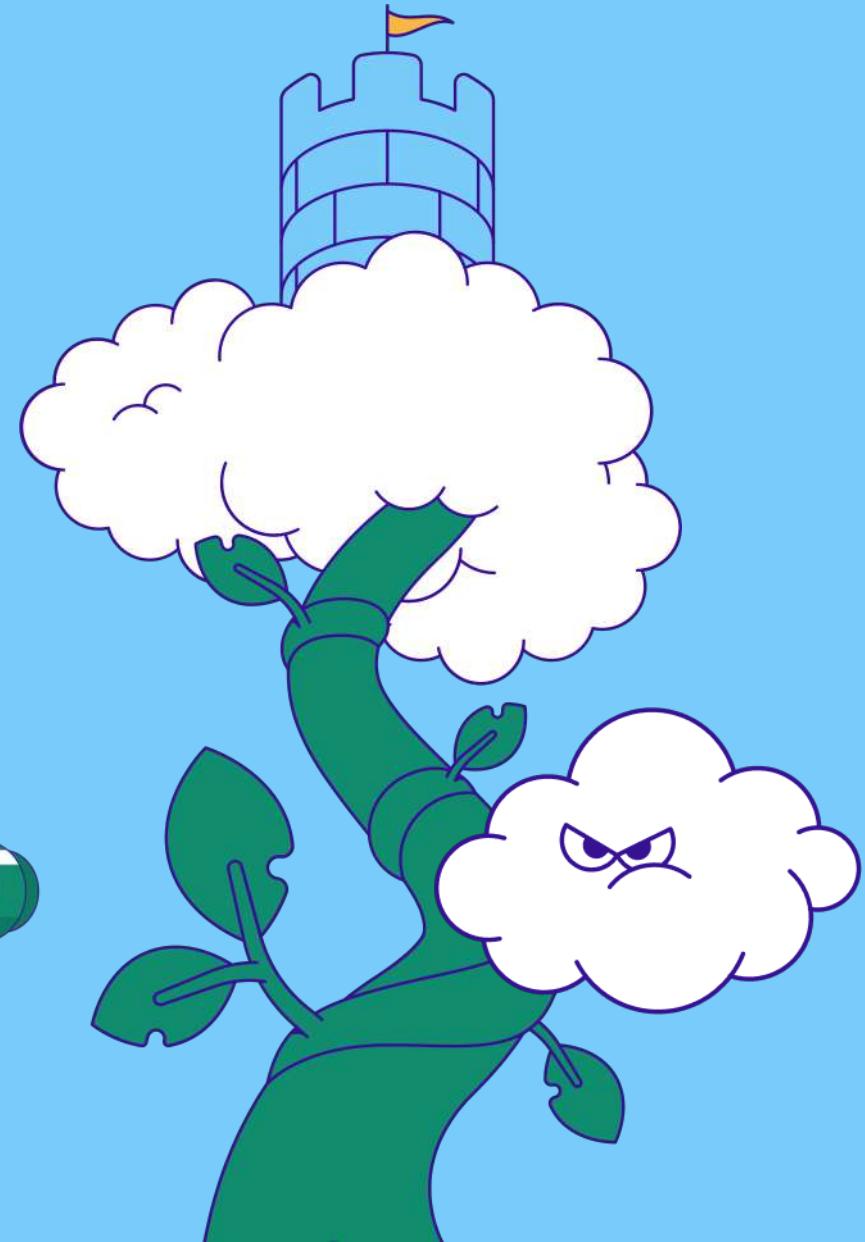


Azure



AGENDA

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



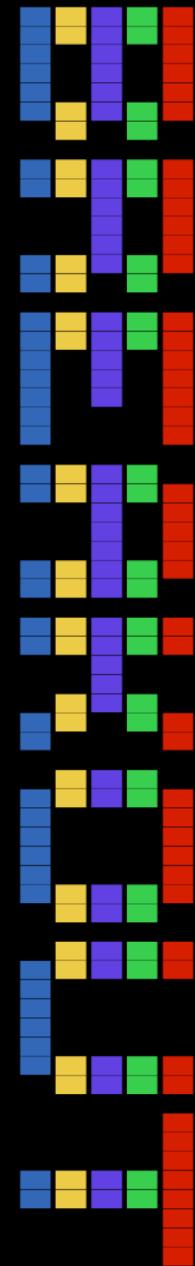
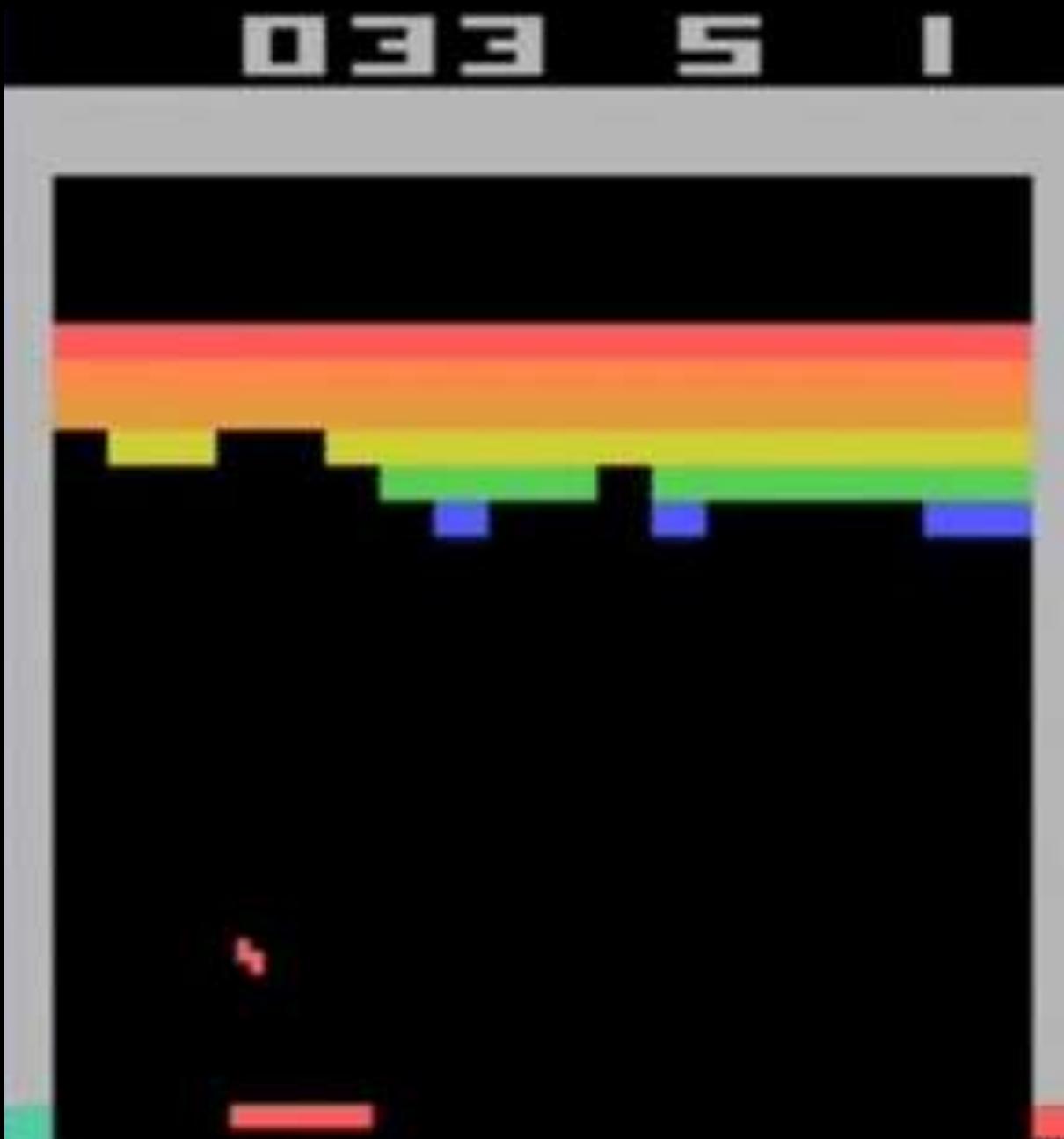
AGENDA

- PROBLEM: Noisy Console Logs 🐞 🐞



ATARI

PERIOD



No Permissions – 1/3 – Console Home

The screenshot shows the AWS Console Home interface in a web browser. The URL is [https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/>](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/). The top navigation bar includes tabs for Services, Search, and Global. A sidebar on the left lists Recently visited services, including IAM (selected), Welcome to AWS, AWS Health, and Cost and usage.

IAM (Current Region): Shows 0 Applications. A red box highlights an "Access denied" 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.](#)"

Cost and usage: Shows 0 Cost and usage. A red box highlights an "Access denied" 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 this, detailed information is shown: User: User, Service: ce, Action: GetCostAndUsage.

At the bottom, there are links for CloudShell, Feedback, and cookie preferences, along with copyright information: © 2024, Amazon Web Services, Inc. or its affiliates.

No Permissions – 1/3 – Console Home

The screenshot shows the AWS Console Home interface. On the left, under 'Recently visited', there is a link to 'IAM'. In the center, under 'Applications (0)', there is a message: 'Access denied. You don't have permission to request access, copy the following text and send it to your AWS administrator.' Below this, there is a 'Create application' button and a search bar. At the bottom of this section, there is a 'Go to myApplications' button. On the right, there are two more 'Access denied' messages for 'ce:GetCostAndUsage' and 'servicecatalog>ListApplications'. These messages also instruct the user to copy the provided text and send it to an AWS administrator. The bottom of the screen shows the AWS footer with links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.



servicecatalog>ListApplications

ce:GetCostAndUsage

No Permissions – 1/3 – Console Home

The screenshot shows the AWS Console Home page with a search bar at the top containing "IAM". The search results are displayed under two main sections: "Services" and "Features".

Services (11)

- 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)

- Groups: IAM feature
- Roles: IAM feature
- Policies: IAM feature

On the right side of the screen, there is a large error message box with a red border and a red "X" icon. The message reads:

Access Denied

You don't have permission to perform this action.

Request access

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

User: User:
Service: ce
Action: GetCostAndUsage

At the bottom of the page, there is a footer with links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.



servicecatalog>ListApplications

ce:GetCostAndUsage

No Permissions – 2/3 – IAM Dashboard

The screenshot shows the AWS IAM Dashboard with three 'Access denied' 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.](#)
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
Action: ListAccessKeys
On resource(s): *

AWS Account

- Access denied**: You don't have permission to `iam>ListAccountAliases`. 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: ListAccountAliases

Quick Links

- My security credentials**: Manage your access keys, multi-factor authentication (MFA) and other credentials.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



`servicecatalog>ListApplications`

`ce:GetCostAndUsage`

No Permissions – 2/3 – IAM Dashboard

The screenshot shows the AWS IAM Dashboard with a sidebar containing 'Identity and Access Management (IAM)' and sections for '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 area displays 'Security recommendations' with three 'Access denied' notifications:

- Action: GetAccountSummary**
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
On resource(s): *
- Action: ListMFADevices**
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
On resource(s): user
- Action: ListAccessKeys**
User: arn:aws:iam::200802171337:user/No_Permissions
Service: iam
On resource(s): user

Each notification includes a 'Copy' button and a link to '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 Dashboard with a sidebar containing '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 displays three 'Access denied' messages:

- Access denied** for the action `iam:ListMFADevices` on resource(s) user. The message states: "You don't have permission to perform this operation. To request access, copy the following text and send it to your AWS administrator." A "Copy" button is present.
- Access denied** for the action `iam:ListAccessKeys` on resource(s) user. The message states: "You don't have permission to perform this operation. To request access, copy the following text and send it to your AWS administrator." A "Copy" button is present.
- Access denied** for the action `iam:GetAccountSummary` on resource(s) *. The message states: "You don't have permission to perform this operation. To request access, copy the following text and send it to your AWS administrator." A "Copy" button is present.

At the bottom, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.



`servicecatalog>ListApplications`

`ce:GetCostAndUsage`

`iam>ListAccountAliases`

`iam:GetAccountSummary`

`iam>ListMFADevices`

`iam>ListAccessKeys`

No Permissions – 2/3 – IAM Dashboard

The screenshot shows the AWS IAM Dashboard with a sidebar containing '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 displays three 'Access denied' messages:

- Service: iam Action: ListMFADevices On resource(s): user**
- Access denied**
You don't have permission to . 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:u ser/No_Permissions
Service: iam
Action: ListAccessKeys
On resource(s): user
- Access denied**
You don't have permission to . 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:u ser/No_Permissions
Service: iam
Action: GetAccountSummary
On resource(s): *



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 Users page. On the left, a sidebar menu is open under 'Access management' with 'Users' selected, indicated by a yellow arrow. The main content area displays a table with one row, showing an 'Access denied' message. The message states: 'You don't have permission to `iam>ListUsers`. To request access, copy the following text and send it to your AWS administrator.' It includes a 'Copy' button and the following details:
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



`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 Users page. The left sidebar is collapsed, and the main content area displays a table with one row. A large red arrow points to the 'Users' link in the sidebar. The table has columns for User name, Path, Groups, Last activity, MFA, and Password. The single row in the table is highlighted with a pink background. An 'Access denied' message box is overlaid on the table, containing the following text:

Access denied
You don't have permission to . 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

At the bottom of the page, there are links for CloudShell and Feedback, and standard footer links for Privacy, Terms, and Cookie preferences.



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 Users page. On the left, a sidebar menu is open under 'Access management' with 'Users' selected, indicated by a yellow arrow. The main content area displays a table header for 'Users (0) Info'. Below the header, a message box shows an 'Access denied' error: 'You don't have permission to [REDACTED] To request access, copy the following text and send it to your AWS administrator.' It includes a 'Copy' button and a detailed error message:
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



No Permissions – 3/3 – IAM Users

Screenshot of the AWS IAM Users page showing three users with no permissions:

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

The screenshot also shows the AWS navigation bar and the IAM service menu.

{

```
"Version": "2012-10-17",
"Statement": [
```

```
{
```

```
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": "iam>ListUsers",
    "Resource": "*"
}
```

```
}
```

```
}
```



No Permissions – 3/3 – IAM Users

Screenshot of the AWS IAM console showing a user with no permissions. The user 'No_Permissions' has three groups assigned, each with 'Access denied' for all actions.

User name	Groups	Last activity	MFA	Password
No_Permissions	Access denied	Access denied	Access denied	Access denied
No_Permissions	Access denied	Access denied	Access denied	Access denied
No_Permissions	Access denied	Access denied	Access denied	Access denied

The error message for the first group states: "You don't have permission to iam>ListGroupsForUser. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)"

Details of the error:

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

{

```
"Version": "2012-10-17",  
"Statement": [
```

{

```
    "Sid": "VisualEditor0",  
    "Effect": "Allow",  
    "Action": "iam>ListUsers",  
    "Resource": "*"
```

}

]

}



Console Mapping – IAM Users

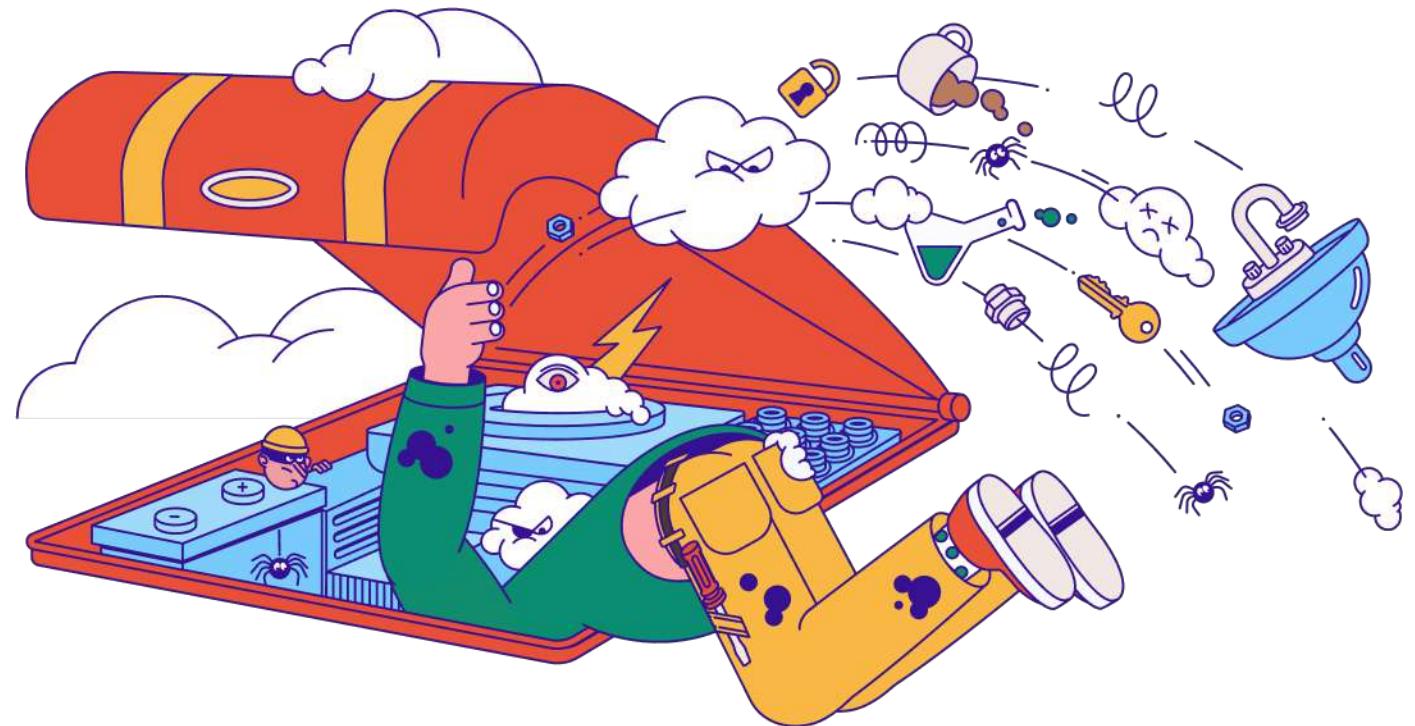


Console Mapping – IAM Users



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

Search

User name	Path	Groups	Last activity	MFA	Password
No_Permissions	/				

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

Copy

B

Users (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

User name	Path	Groups	Last activity	MFA	Password
Andi_Ahmeti	/	1	-	-	-
Daniel_Bohannon	/	1	-	-	-
No_Permissions	/	0	5 hours ago	Virtual	-

C

Users (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

User name	Path	Groups	Last activity	MFA	Password
Andi_Ahmeti	/	1	-	-	-
Daniel_Bohannon	/	1	-	-	-
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}	

C

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



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:ListSigningCertificates	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:17.0000	iam>ListMFADevices	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:18.0000	iam>ListGroupsForUser	aws-internal/3 aws-sdk-java/...		AccessDenied
2024-03-18 04:17:19.0000	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

C

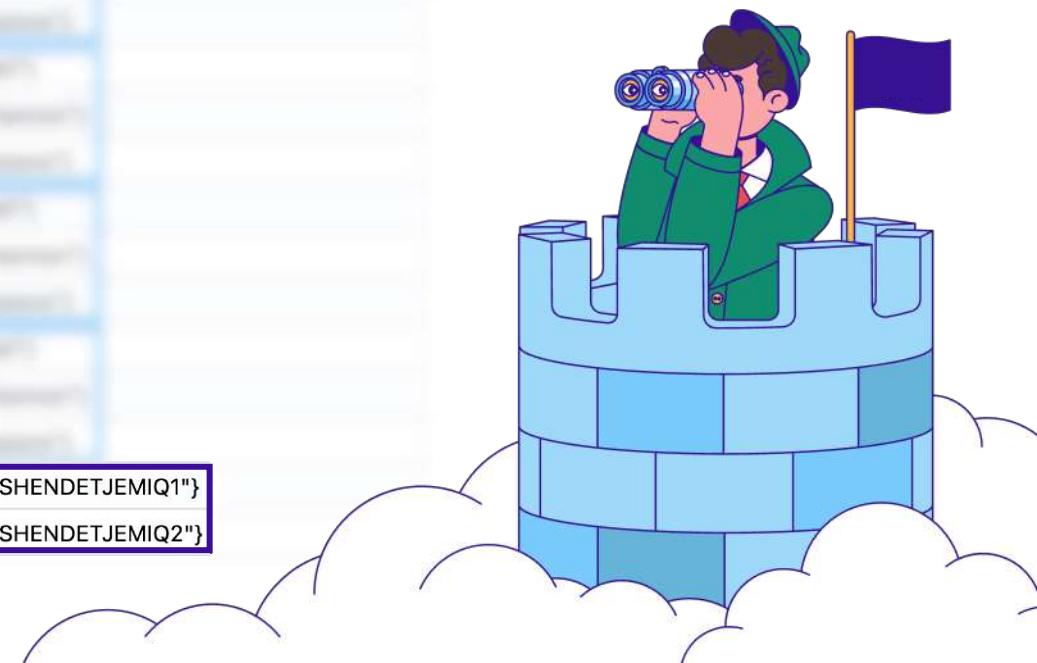
eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:20:50.0000	iam>ListUsers	AWS Internal	{"maxItems":1000}	
2024-03-18 04:20:51.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Andi_Ahmeti"}	
2024-03-18 04:20:51.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...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



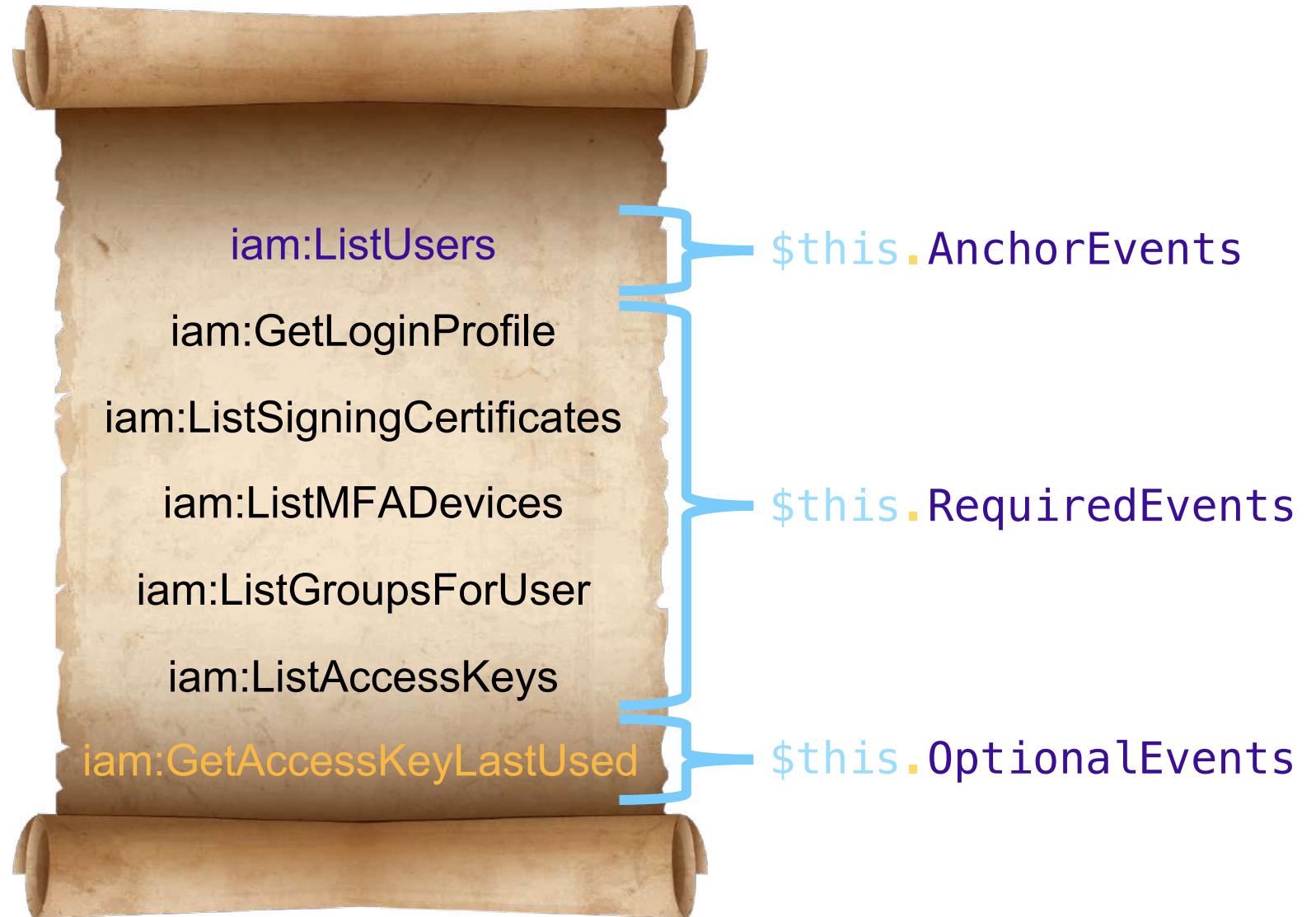
Console Mapping – IAM Users

A
C

iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}

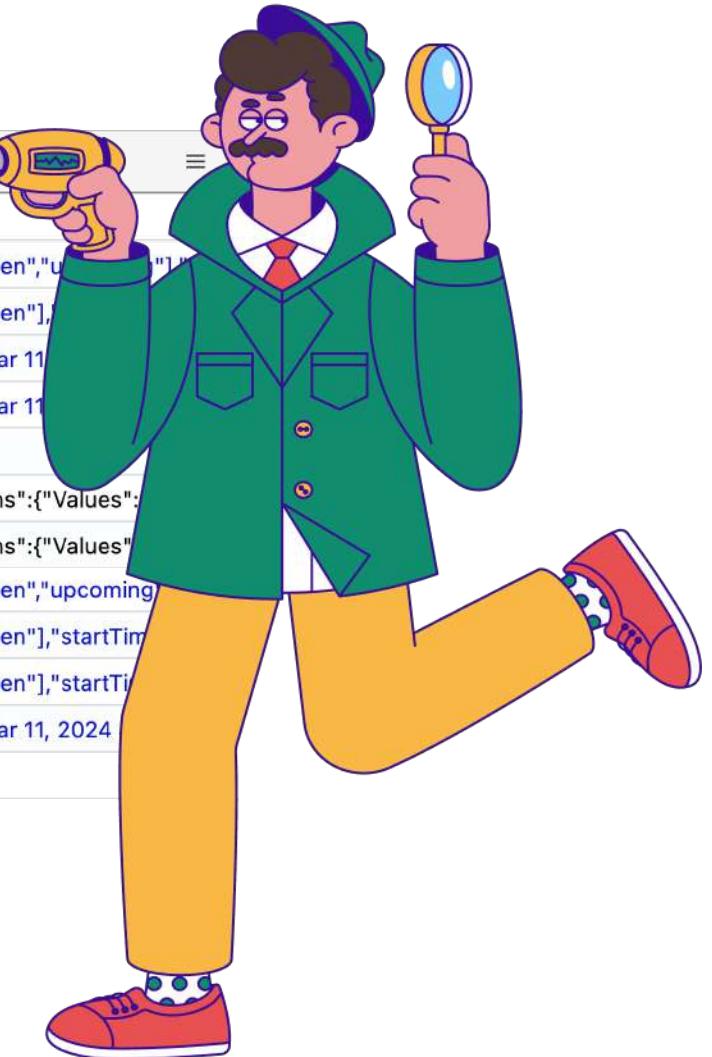


Console Mapping – IAM Users



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 04:19:43.0000	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"]}}
2024-03-18 04:19:43.0000	health:DescribeEventAggregates	Mozilla/5.0 (Macintosh; Intel ...	{"filter":{"startTimes":[{"from":"Mar 11, 2024"}]}}
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	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"],"startTimes":[]}}
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"eventStatusCodes":["open"],"startTimes":[]}}
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":{"Name":"CostCenter","Value":...}}]}}
2024-03-18 04:19:44.0000	ce:GetCostForecast	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":[{"Dimensions":{"Name":"CostCenter","Value":...}}]}}
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"}]}
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"],"startTimes":[{"from":"Mar 11, 2024"}]}}
2024-03-18 04:19:44.0000	health:DescribeEventAggregates	health.amazonaws.com	{"filter":{"eventStatusCodes":["open"],"startTimes":[{"from":"Mar 11, 2024"}]}}
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":{},"Comparison":">C	
2024-03-18 04:19:44.0000		ce:GetCostForecast		Mozilla/5.0 (Macintosh; Intel ...		{"Filter":{"Not":{"Or":[{"Dimensions":{},"Comparison":">C	
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 00:00:00 UTC"}]}	
2024-03-18 04:19:43.0000		health:DescribeEventAggregates		health.amazonaws.com		{"filter":{"startTimes":[{"from":"Mar 11, 2024, 00:00:00 UTC"}]}	
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","upcomin	
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 00:00:00 UTC"}]}}	



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":{"Value": "C...","C...": "C..."}]}]}
2024-03-18 04:19:44.0000	ce:GetCostForecast	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":[{"Dimensions":{"Value": "C...","C...": "C..."}]}]}
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 – OptionalEvents (Context)

Screenshot of the AWS IAM User console showing the user "Everything_Bagel".

Identity and Access Management (IAM)

Everything_Bagel

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.

Permissions | Groups (1) | Tags (5) | Security credentials | Access Advisor

Permissions policies (4)

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

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM console showing the permissions for a user named "Everything_Bagel".

The left sidebar shows the navigation menu for Identity and Access Management (IAM), including sections for 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 displays the "Permissions" tab under "Identity and Access Management (IAM)". It shows "Permissions policies (4)" attached to the user:

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, there is a section for "Permissions boundary (set)". It allows setting a permissions boundary to control the maximum permissions for this user. A boundary named "AdministratorAccess" is listed, which is an AWS managed - job function. Buttons for "Change boundary" and "Remove boundary" are available.

At the bottom of the page, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM Groups page showing a user group named "newUserGroupWith3PoliciesAdded".

The page displays the following information:

- User groups membership (1)**: A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.
- Attached policies**: AmazonEC2SpotFleetTaggingRole, AWSQuickSightListIAM an...

The left sidebar shows the following navigation paths:

- 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)
- Related consoles
 - IAM Identity Center
 - AWS Organizations

Page footer:

- CloudShell
- Feedback
- © 2024, Amazon Web Services, Inc. or its affiliates.
- Privacy
- Terms
- Cookie preferences



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM console showing the Tags section. The URL is https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/tags.

The left sidebar shows the Identity and Access Management (IAM) navigation menu. The Tags section is currently selected.

The main content area displays a table of tags:

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



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM console showing the Security credentials page for a user named "Everything_Bagel".

The page displays the following information:

- Console sign-in:** Includes a "Console sign-in link" (https://200802171337signin.aws.amazon.com/console) and a "Console password" updated 2 hours ago.
- Multi-factor authentication (MFA):** Shows one assigned MFA device: "Virtual" type, Identifier "arn:aws:iam::200802171337:mfa/ExampleMFADevice", and status "Not Applicable".
- Access keys:** Shows two access keys: "AKIAPERSHENDETJEMIQ1" (Status: Active, Last used: None, Created: 2 hours ago).

The left sidebar shows the navigation menu for IAM, including "Identity and Access Management (IAM)", "Access management", "Access reports", and "Related consoles".



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM console showing two access keys and an SSH public key.

Access keys (2)

Access Key ID	Description	Status
AKIAPERSHENDETJEMIQ1	myFirstTag	Active
AKIAPERSHENDETJEMIQ2	mySecondTag	Active

SSH public keys for AWS CodeCommit (5)

SSH Key ID	Uploaded	Status
Key 1	2024-01-01 12:00:00 UTC	Active
Key 2	2024-01-01 12:00:00 UTC	Active
Key 3	2024-01-01 12:00:00 UTC	Active
Key 4	2024-01-01 12:00:00 UTC	Active
Key 5	2024-01-01 12:00:00 UTC	Active



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM console showing the SSH public keys, HTTPS Git credentials, and Credentials for Amazon Keyspaces sections.

SSH public keys for AWS CodeCommit (5)

SSH Key ID	Uploaded	Status
APKAPERSHENDETJEMIQ1	2 days ago	Active
APKAPERSHENDETJEMIQ2	2 days ago	Active
APKAPERSHENDETJEMIQ3	2 days ago	Active
APKAPERSHENDETJEMIQ4	2 days ago	Active
APKAPERSHENDETJEMIQ5	2 days ago	Active

HTTPS Git credentials for AWS CodeCommit (1)

User name	Created	Status
Everything_Bagel-at-200802171337	2 days ago	Active

Credentials for Amazon Keyspaces (for Apache Cassandra) (2)

User name	Created	Status
Everything_Bagel-at-200802171337	2 days ago	Active
Everything_Bagel+1-at-200802171337	2 days ago	Active



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM console showing the 'OptionalEvents' context mapping feature.

The left sidebar shows the navigation menu for IAM:

- Identity and Access Management (IAM) (selected)
- Dashboard
- Access management
 - User groups
 - Users** (selected)
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access Analyzer
 - External access
 - Unused access
 - Analyzer settings
 - Credential report
 - Organization activity
 - Service control policies (SCPs)
- Related consoles
 - IAM Identity Center
 - AWS Organizations

The main content area displays four sections of optional events:

- HTTPS Git credentials for AWS CodeCommit (1)**: Generates credentials for AWS CodeCommit. One entry is listed:

User name	Created	Status
Everything_Bagel-at-200802171337	2 days ago	Active
- Credentials for Amazon Keyspaces (for Apache Cassandra) (2)**: Generates credentials for Amazon Keyspaces (Apache Cassandra). Two entries are listed:

User name	Created	Status
Everything_Bagel-at-200802171337	2 days ago	Active
Everything_Bagel+1-at-200802171337	2 days ago	Active
- X.509 Signing certificates (1)**: Manages X.509 certificates. One entry is listed:

Creation time	Thumbprint	Status
2 days ago	SHQIP1FUN2ME3MIRE4VONE5SE6KURRE7	Active

At the bottom, there are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM console showing the user "Plain_Bagel".

Identity and Access Management (IAM)

Plain_Bagel

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)

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

Filter by Type

Policy name	Type	Attached via
No resources to display		

Related consoles

IAM Identity Center AWS Organizations

CloudShell **Feedback**

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



Console Mapping – OptionalEvents (Context)

Screenshot of the AWS IAM User console showing the "Plain_Bagel" user details. The user was created on February 16, 2024, at 02:06 UTC-05:00. It has console access disabled and one access key.

Summary

ARN	Console access	Access key 1
arn:aws:iam::200802171337:user/Plain_Bagel	Disabled	Create access key

Permissions

Permissions policies (0)

No resources to display

Permissions boundary (not set)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



Console Mapping – OptionalEvents (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":"AAI1zjUVlnJUxBcsOtgybPoPxBF...}	
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 – 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	iamListGroupPolicies	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	iamListGroupPolicies	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	iamGetLoginProfile	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	iamGetAccessKeyLastUsed	AWS Internal	{"accessKeyId": "AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:44.0000	iamGetAccessKeyLastUsed	AWS Internal	{"accessKeyId": "AKIAPERSHENDETJEMIQ2"}
	2024-03-18 04:24:45.0000	iamGetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId": "AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:45.0000	iamGetAccessKeyLastUsed	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	iamListGroupPolicies	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	iamGetLoginProfile	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	iamGetAccessKeyLastUsed	AWS Internal	{"accessKeyId": "AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:44.0000	iamGetAccessKeyLastUsed	AWS Internal	{"accessKeyId": "AKIAPERSHENDETJEMIQ2"}
	2024-03-18 04:24:45.0000	iamGetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId": "AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:45.0000	iamGetAccessKeyLastUsed	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 – OptionalEvents (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:GetPolicy	
iam>ListPolicies		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 – OptionalEvents (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:GetPolicy
iamListGroupPolicies
iamListAttachedGroupPolicies
iamGetAccessKeyLastUsed

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

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



Console Mapping – OptionalEvents (Context)



Permissions Groups Tags **Security credentials** Access Advisor



iam>ListPolicies

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 – OptionalEvents (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 – OptionalEvents (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:GetPolicy
iamListGroupPolicies
iamListAttachedGroupPolicies
iamGetAccessKeyLastUsed

iamGetAccessKeyLastUsed
iamGetAccessKeyLastUsed

Console Mapping – OptionalEvents (Context)



iam>ListPolicies

Permissions Groups Tags Security credentials Access Advisor

eventNameFull	≡
iam>ListAccessKeys	
iam>ListSigningCertificates	
iam>ListSSHPublicKeys	
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": "AIDA12345678ABCDEFGH",
    "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

The terminal window displays the AWS CLI interface with the following commands and their outputs:

- Step 1:** `aws iam create-user --user-name krileva`
Output: A JSON object representing the newly created IAM user "krileva".

```
bash-3.2$ bash-3.2$ aws iam create-user --user-name krileva
{
  "User": {
    "Path": "/",
    "UserName": "krileva",
    "UserId": "AIDA12345678ABCDEFGH",
    "Arn": "arn:aws:iam::200802171337:user/krileva",
    "CreateDate": "2024-03-22T03:48:59+00:00"
  }
}
bash-3.2$
```
- Step 2:** `aws iam create-access-key --user-name krileva`
Output: A JSON object representing the access key for the user "krileva".

```
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$
```
- Step 3:** `aws iam attach-user-policy --user-name krileva --policy-arn arn:aws:iam::aws:policy/AdministratorAccess`
Output: Confirmation of the policy attachment.

```
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



```
aws-3.2$ bash-3.2$ aws iam create-user --user-name krileva
{
  "User": {
    "Path": "/",
    "UserName": "krileva",
    "UserId": "AIDA12345678ABCDEFGH",
    "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

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)  
  
{'Arn': 'arn:aws:iam::200802171337:user/krileva',  
 'CreateDate': datetime.datetime(2024, 3, 22, 4, 52, 49, tzinfo=tzutc()),  
 'Path': '/',  
 'UserId': 'AIDA12345678ABCDEFGH',  
 '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

```
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 response = iam_client.attach_user_policy(UserName=username,PolicyArn=policyArn)  
25 print(f"\niam_client.attach_user_policy(UserName={username},PolicyArn={policyArn})\n")  
26
```

1

2

3

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$  
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': 'AIDA12345678ABCDEFGH',  
 'UserName': 'krileva'}  
  
1  
  
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'}  
  
2  
  
iam_client.attach_user_policy(UserName=krileva,PolicyArn=arn:aws:iam::aws:policy/AdministratorAccess)  
  
3  
  
bash-3.2$
```

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")  
pprint (response['AccessKey'])  
  
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20
```

CLI vs Console



A screenshot of the AWS Identity and Access Management (IAM) console in a web browser. The URL is <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/users>. The browser window has a tab labeled "Users | IAM | Global". The left sidebar shows the "Identity and Access Management (IAM)" navigation pane with options like Dashboard, 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 "Users (3) Info" and contains a table with three rows:

User name	Path	Groups	Last activity	MFA	Password
Andi_Ahmeti	/	1	-	-	-
Daniel_Bohannon	/	1	-	-	-
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

eventNameF

parameters

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

eventName	meters

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 04:55:34.0000	iam>GetAccessKey	aws-internal/3 aws-sdk-java/...	{"KeyId":"AKIAPERSHENDETJEMIQ1"}
2024-03-22 04:55:34.0000	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	sso: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

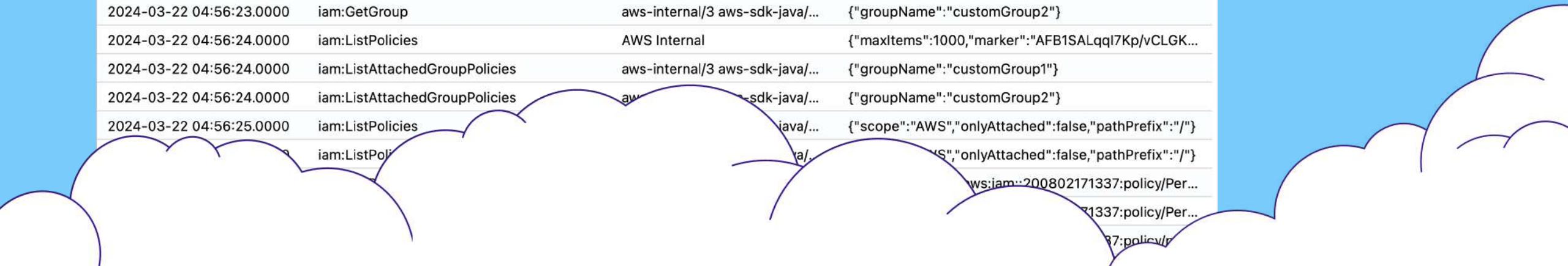
1

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>ListGroups	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":"AFB1SALqqI7Kp/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":"/"} aws:iam::200802171337:policy/Per...
	iam:ListPolicy	aws-internal/3 aws-sdk-java/...	"S","onlyAttached":false,"pathPrefix":"/"} aws:iam::200802171337:policy/Per...
	iam:ListPolicy	aws-internal/3 aws-sdk-java/...	1337:policy/Per...
	iam:ListPolicy	aws-internal/3 aws-sdk-java/...	87:policy/r...

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>ListGroups	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":"AFB1SALqqI7Kp/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

Create

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

15

8

10

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	aws-sdk-java/1.12.100	{"userName":"krileva"}
2024-03-22 04:58:00.0000	iam ListAccessKeys	java/1.8.0_312	{"userName":"krileva"}
			;"arn:aws:iam::200802171337:user/kri...

access-analyst

CLI vs Console



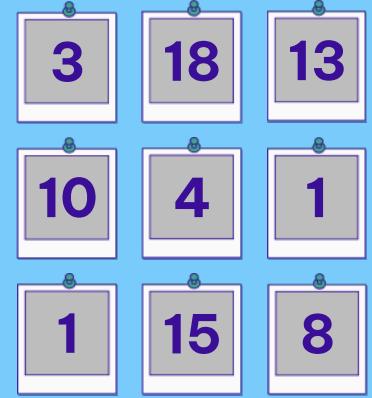
IAM_Users_SPECIFICUSER_CreateAccessKey

eventTime	eventNameFull	userAgent	requestParameters	1	3	18	13
2024-03-22 04:58:57.0000	iam>CreateAccessKey	AWS Internal	{"userName":"krileva"}	1	3	18	13
				10	4	1	
				15	8		

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



CLI vs Console



Worst Case Scenarios



$n=3$

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

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

1

+

5n

+

[0,2n]

1

+

5(3)=15

+

[0,2(3)]=2

18

Worst Case Scenarios



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



$n=20$

Page size
 20 rows
 50 rows
 100 rows

IAM_Users

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",...]

$$21+4(100)=\boxed{421}$$

In Summary...



#Aggregation

In Summary...

IAM_Users_CreateUser

IAM_Users

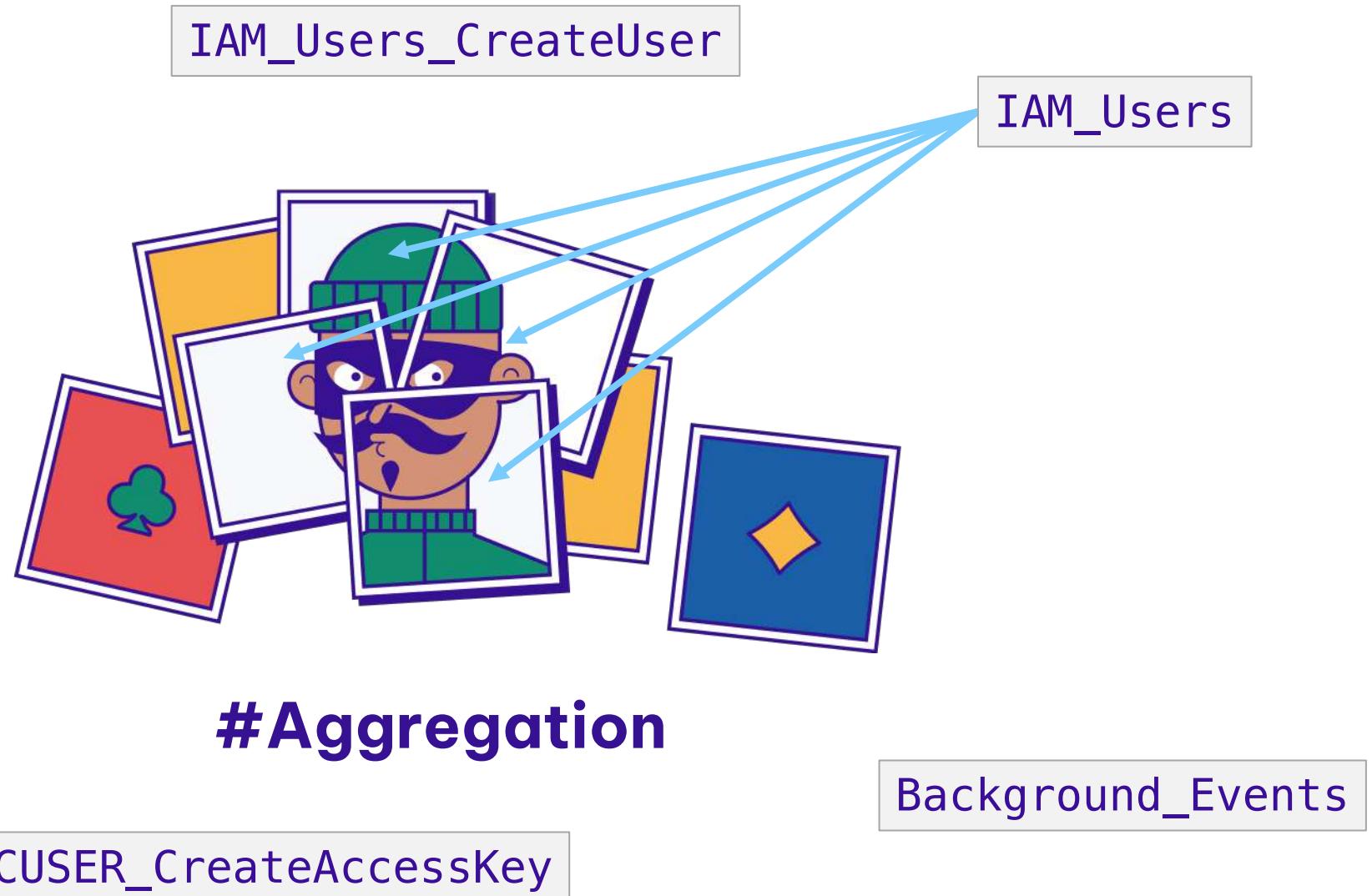


#Aggregation

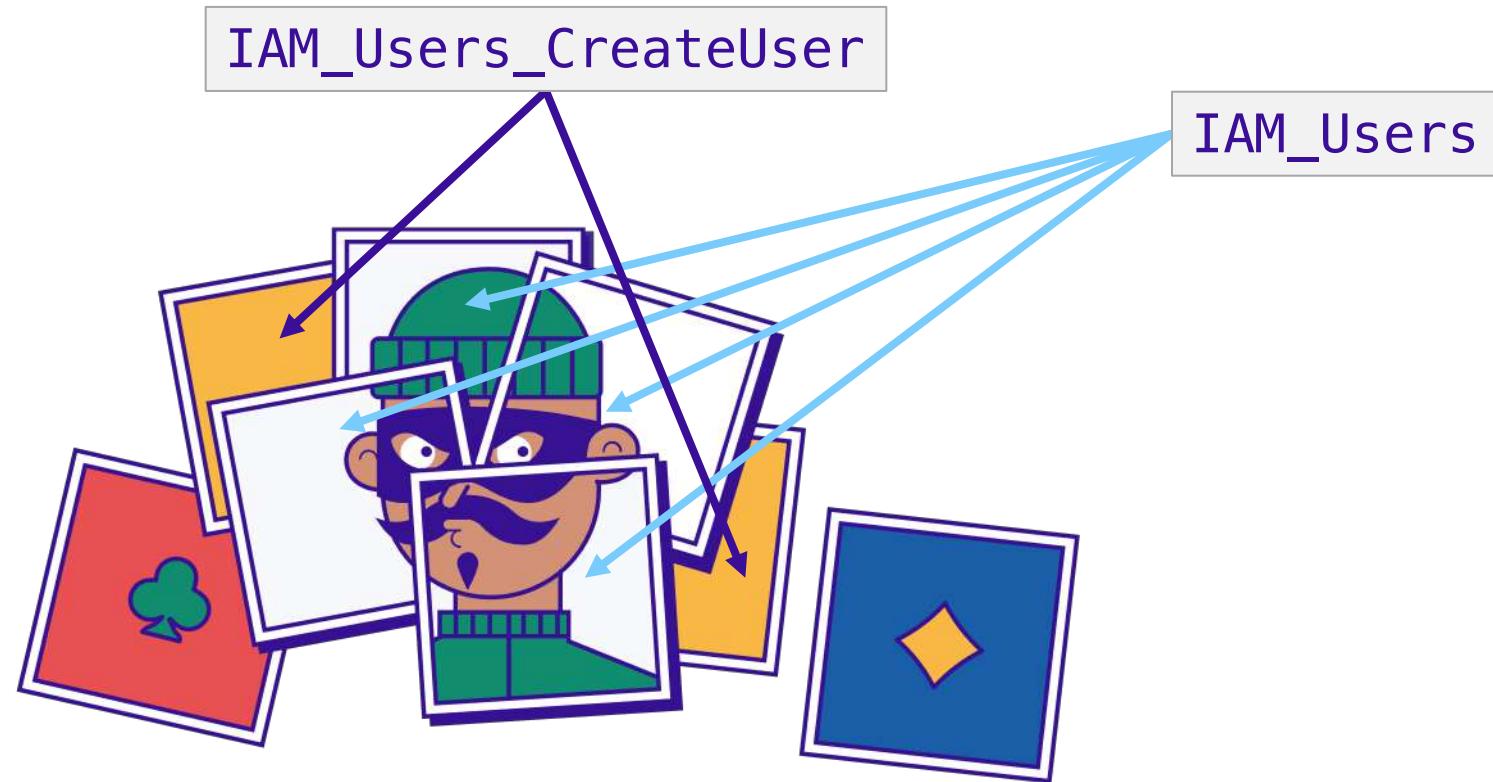
Background_Events

IAM_Users_SPECIFICUSER_CreateAccessKey

In Summary...



In Summary...

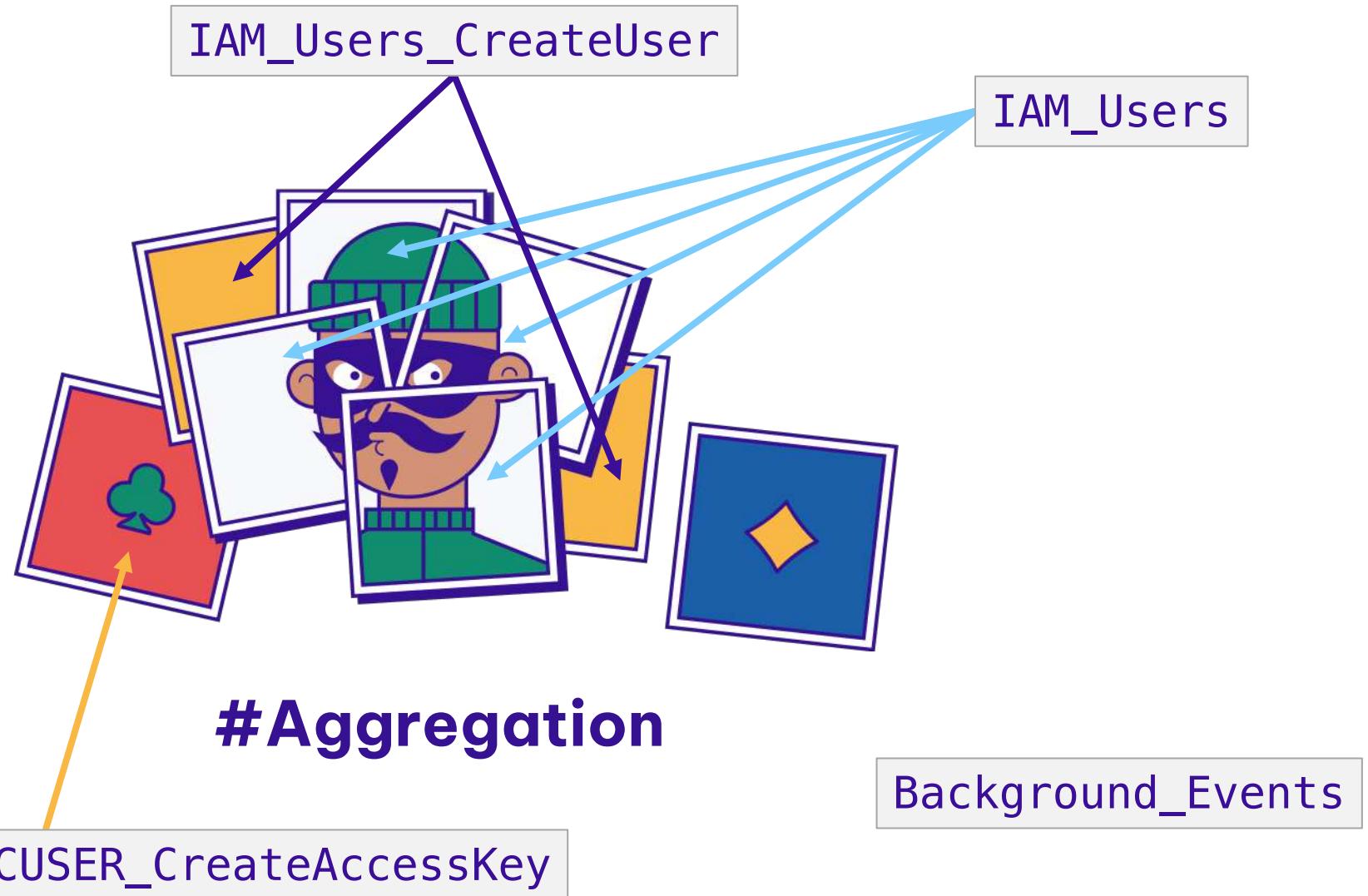


#Aggregation

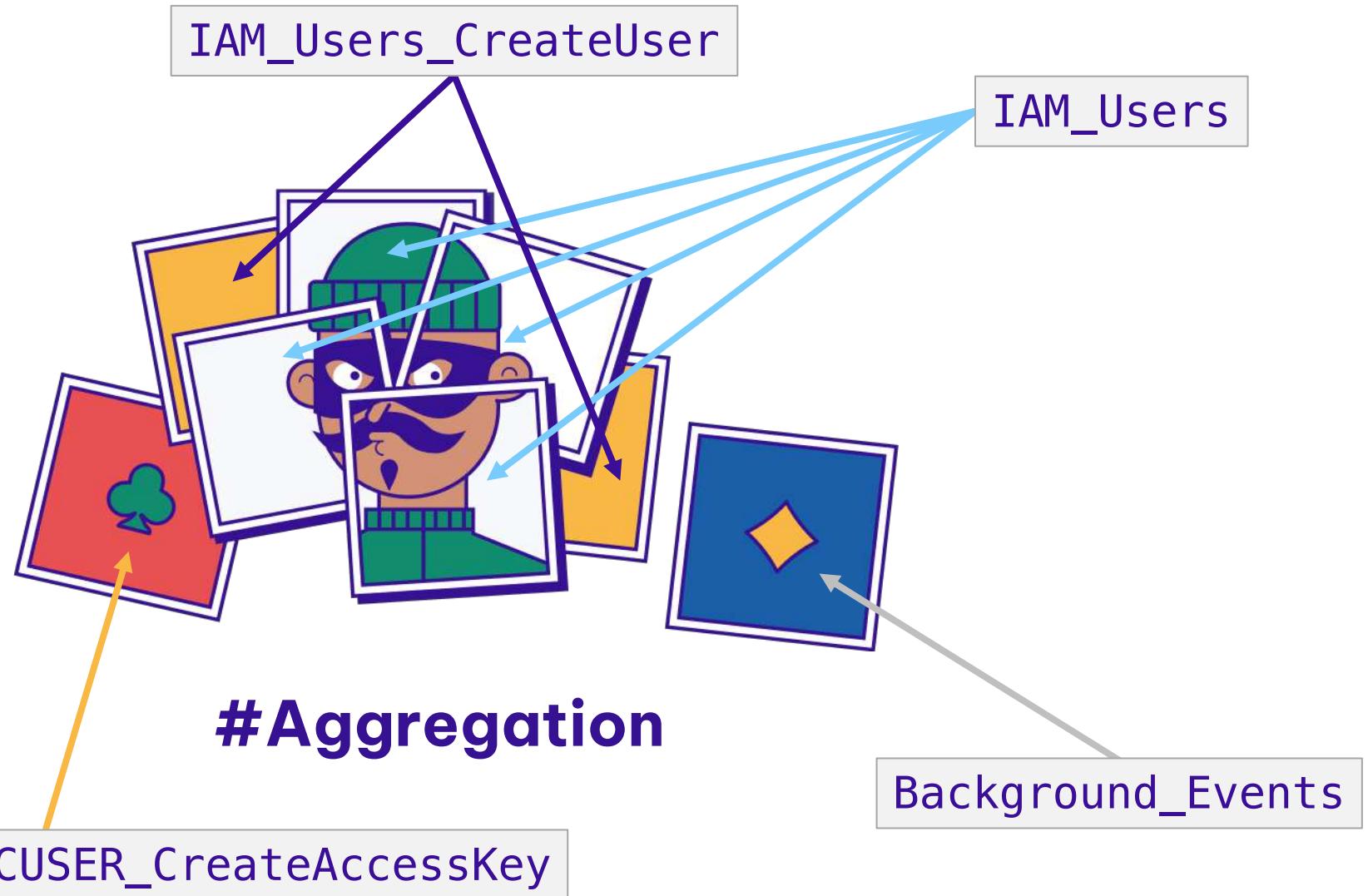
Background_Events

IAM_Users_SPECIFICUSER_CreateAccessKey

In Summary...

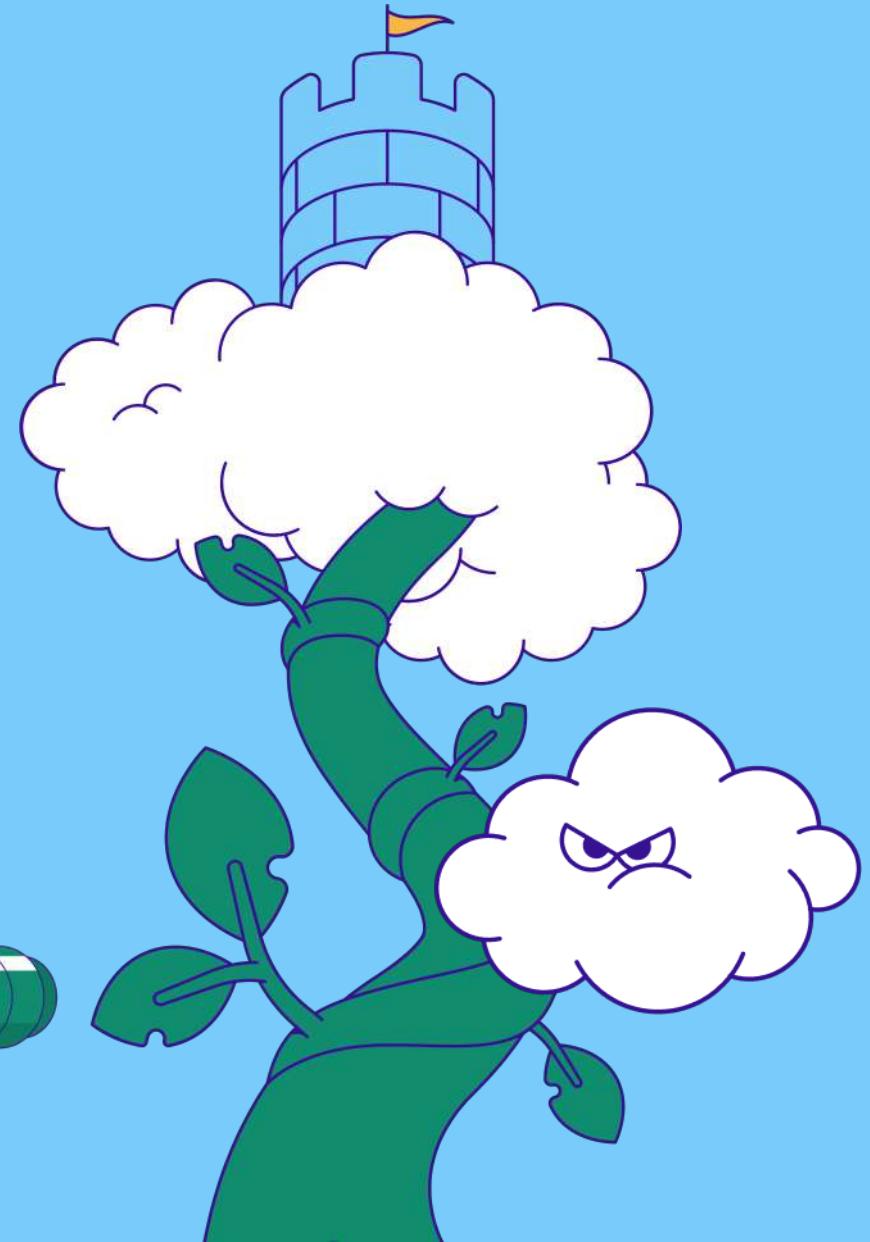


In Summary...

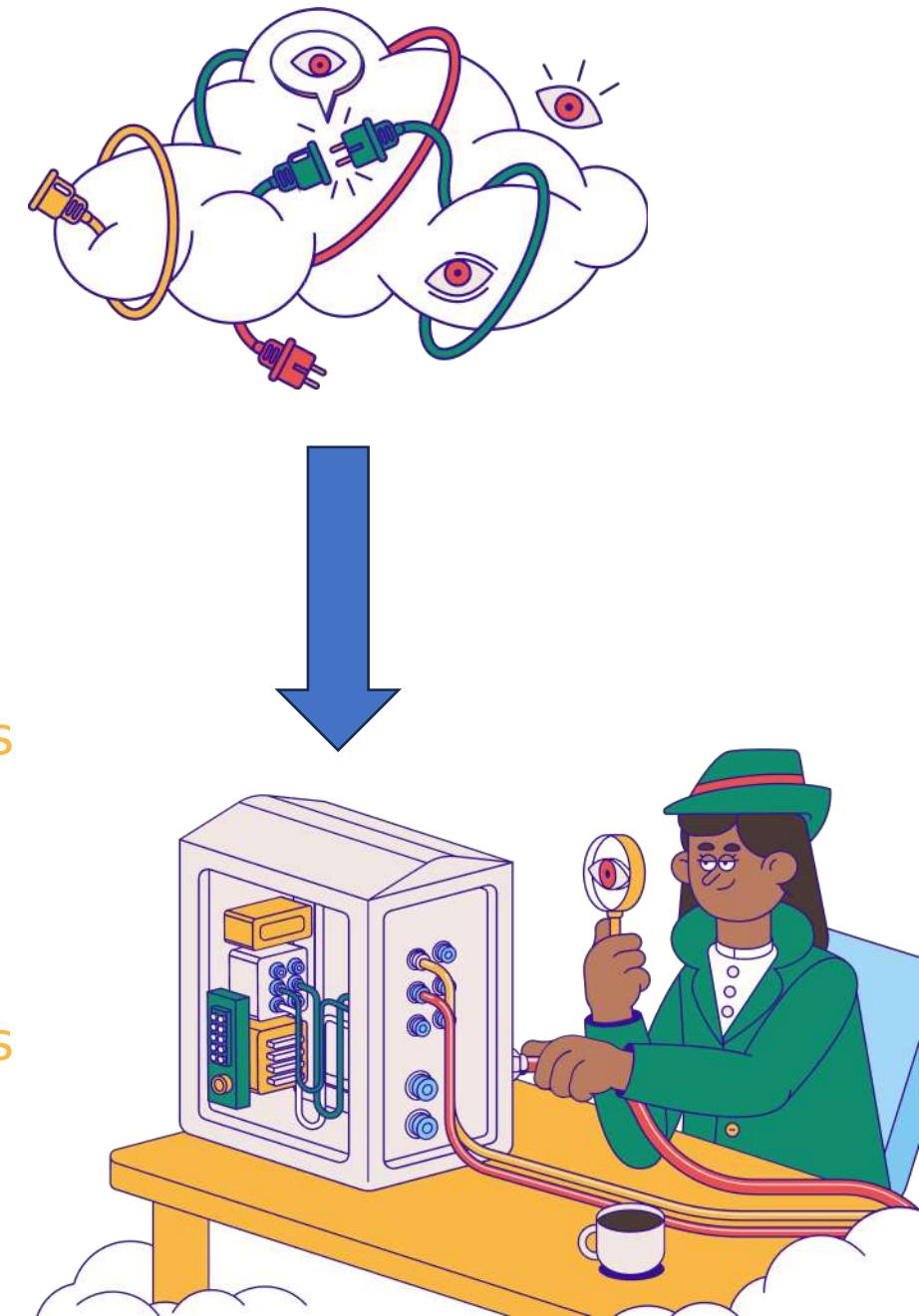


AGENDA

- **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)

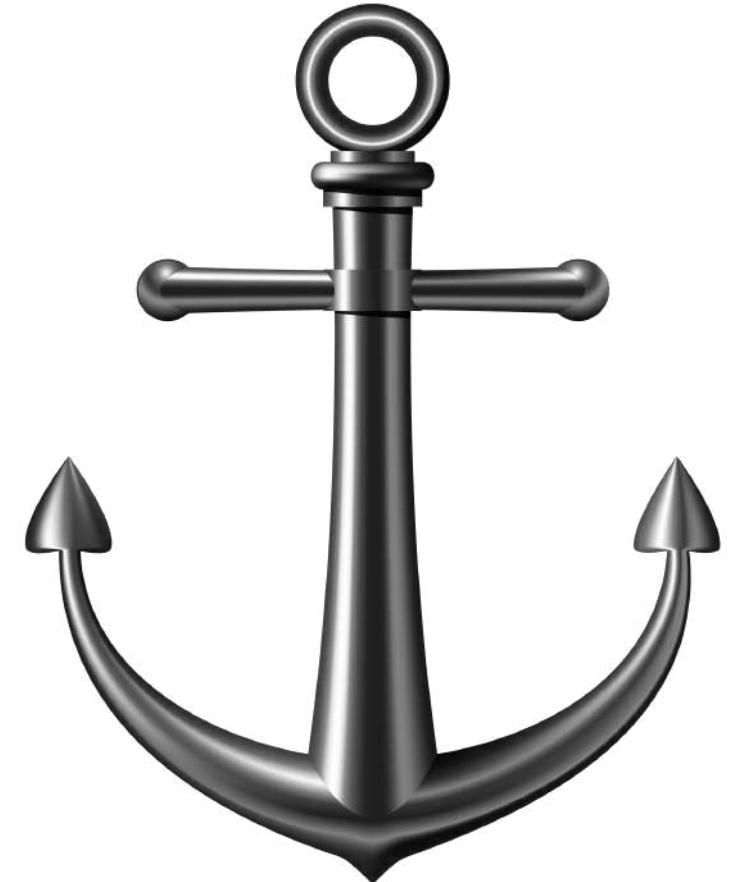
```
'ListUsers' {
    # E.g. {"maxItems":1000}
    if (
        $requestParametersStr -ceq '{"maxItems":1000}' -and `

        $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



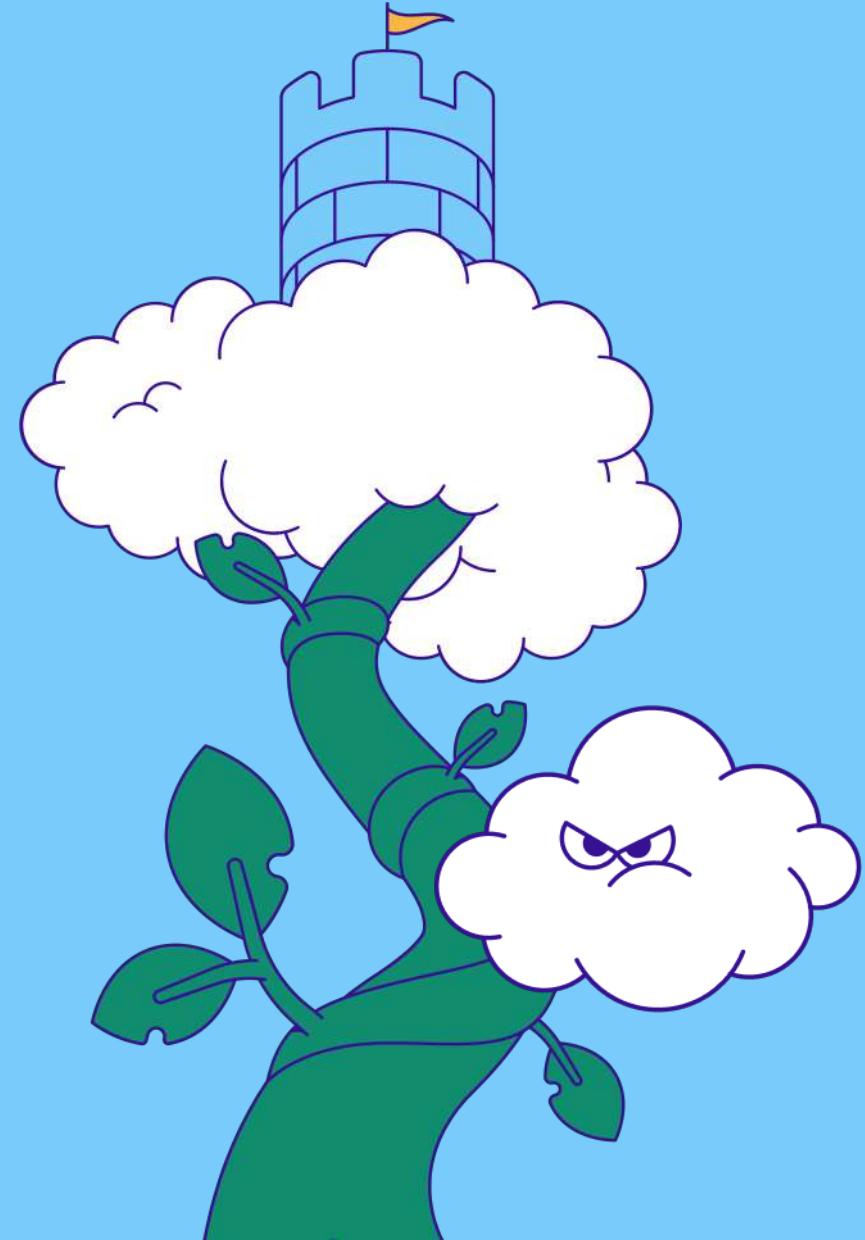
Add'l Cool Tricks & Capabilities

- 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

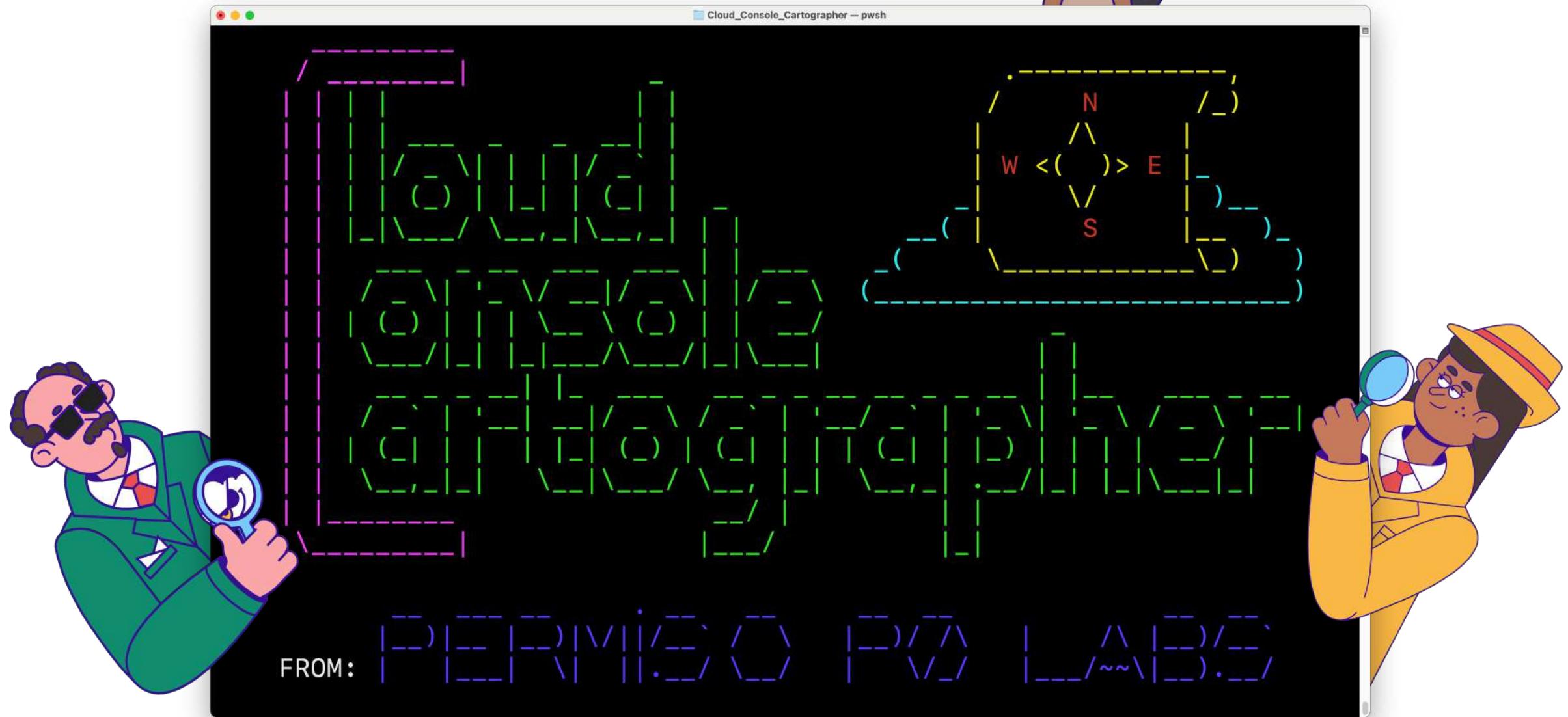


AGENDA

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



DEMO + Public Tool Release

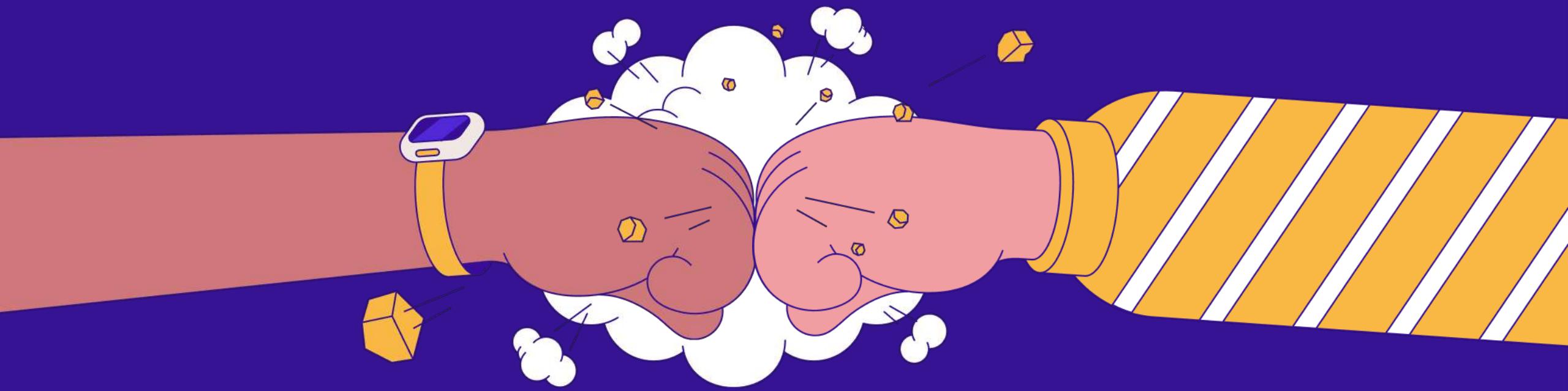


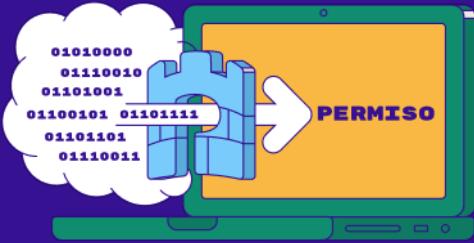
Black Hat Sound Bytes

1. Threat actors continue to use **interactive console UIs** (instead of CLIs) throughout many stages of the attack lifecycle
2. Configure the necessary cloud logging options for retention, forwarding & querying capabilities required to detect & analyze suspicious console session logs
3. Use **Cloud Console Cartographer**, a brand new open-source framework to automatically translate 1000's of events to 10's of mapped "clicks" performed by users in interactive console sessions

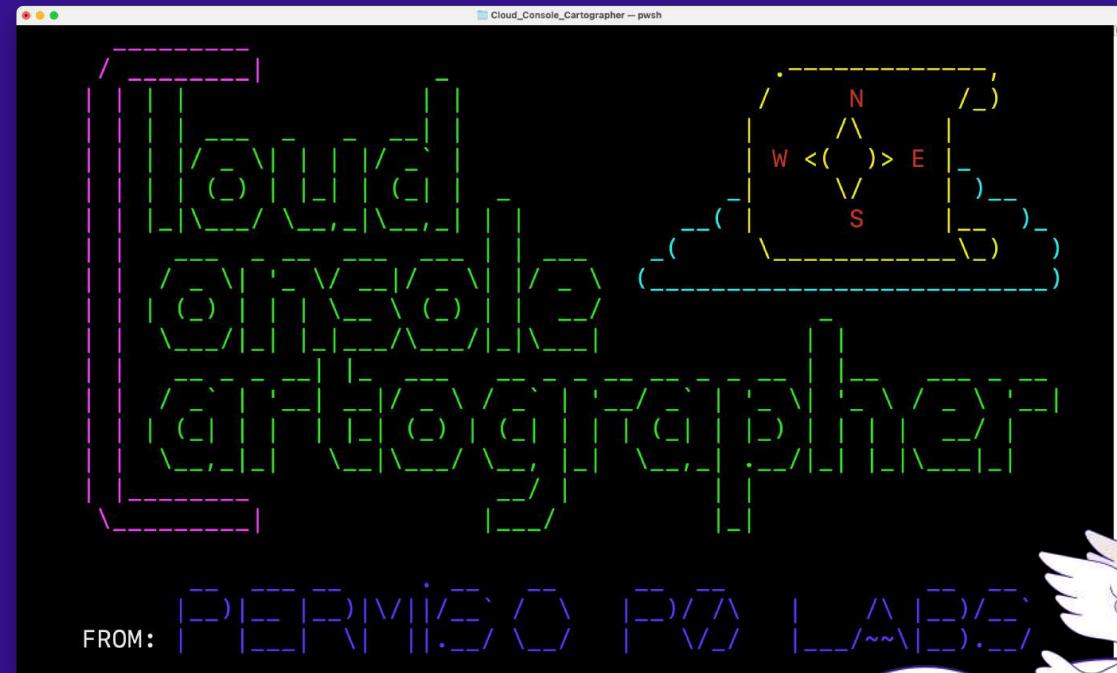


THANKS FOR YOUR TIME!





PERMISO



**ANDI
AHMETI**

andi-ahmeti



danielhbohannon



@danielhbohannon



**DANIEL
BOHANNON**

@SecEagleAnd1



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