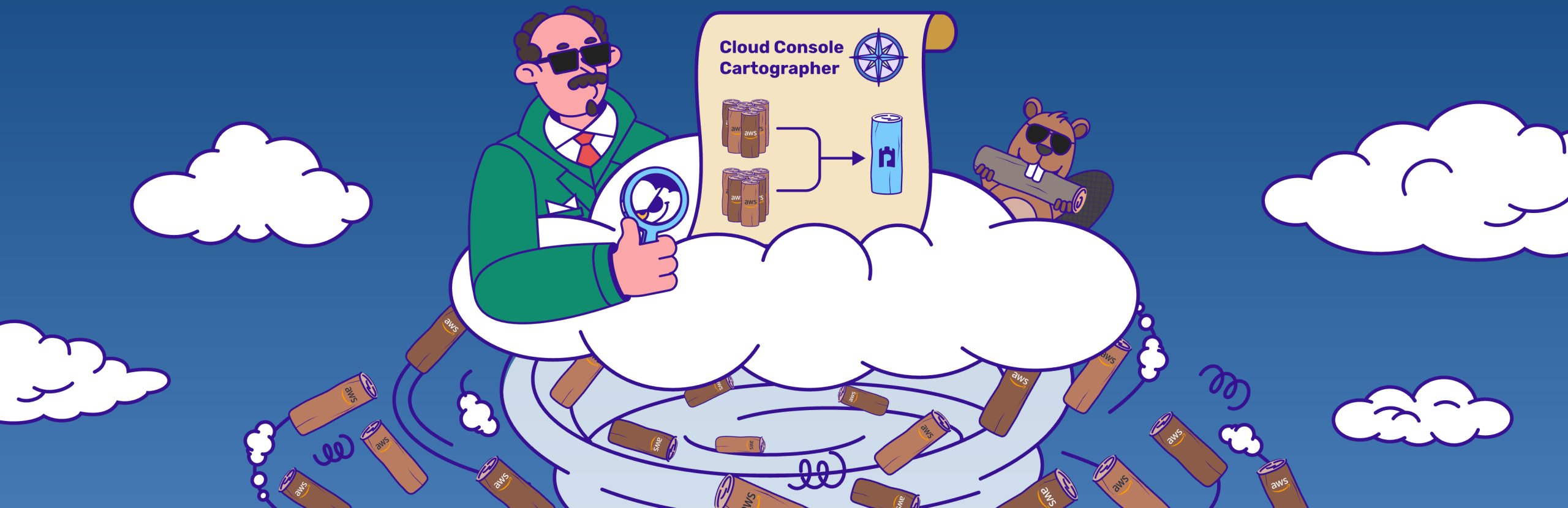
PERMISO

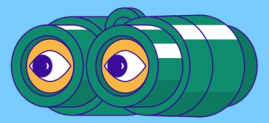
black hat ASIA 2024

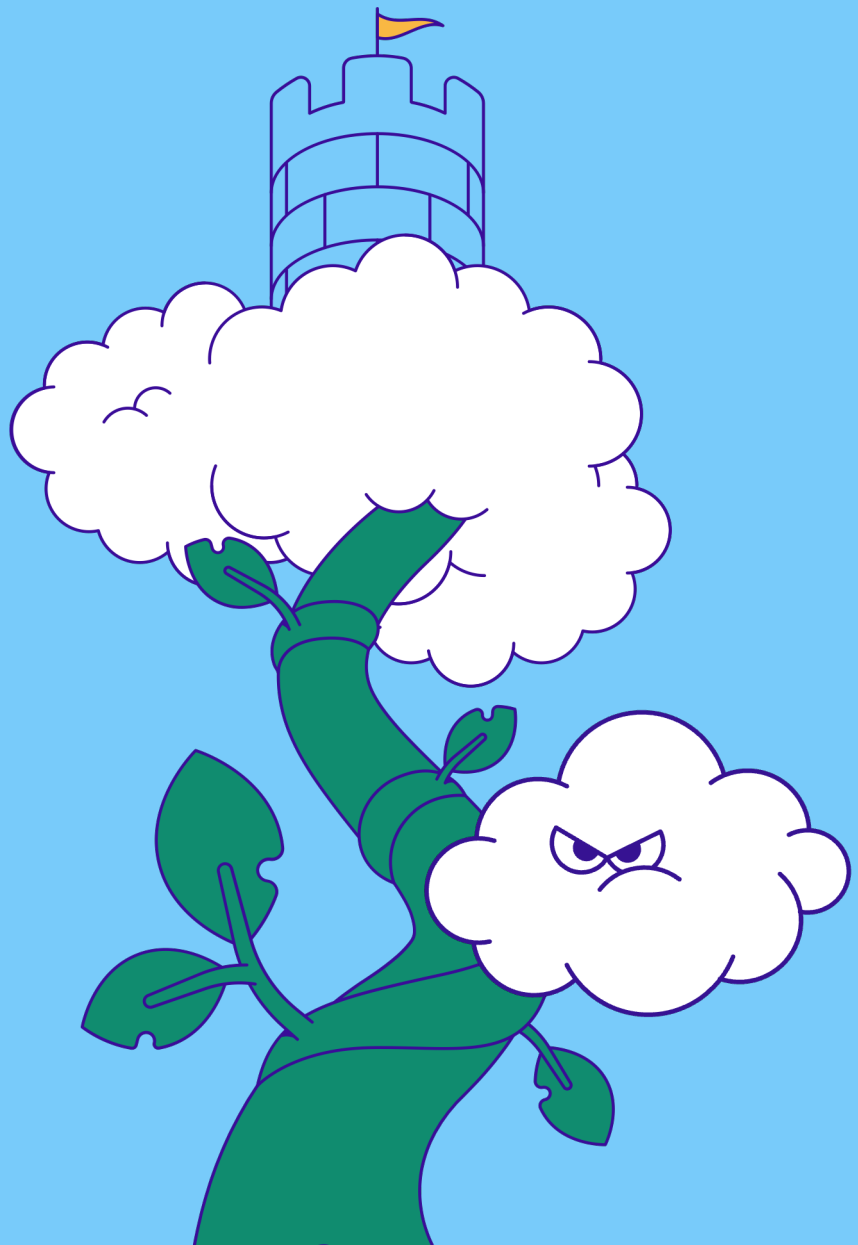
Cloud Console Cartographer

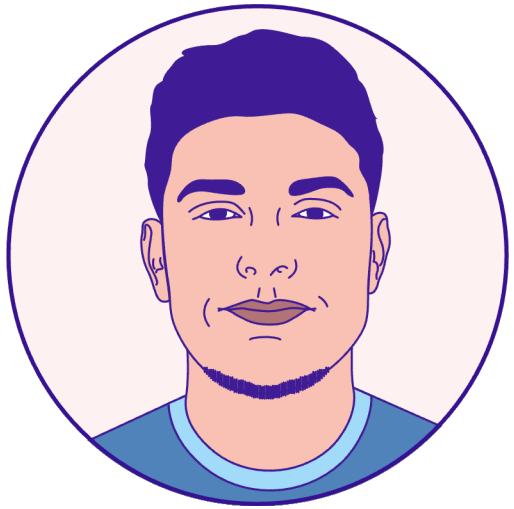
Tapping Into Mapping > Slogging Thru Logging



AGENDA

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





ANDI AHMETI

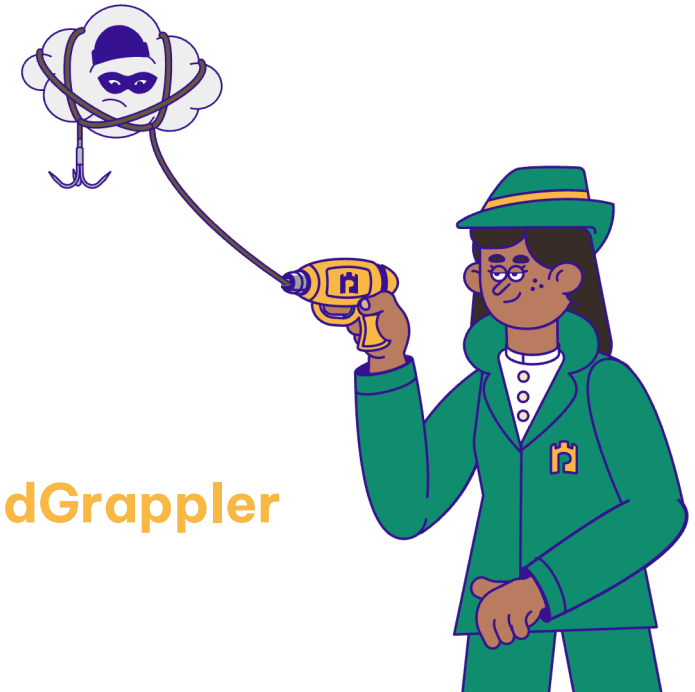
ASSOCIATE THREAT RESEARCHER

Kosovo

@SecEagleAnd1

andi-ahmeti

Permiso-io-tools/**CloudGrappler**



DANIEL BOHANNON

PRINCIPAL THREAT RESEARCHER

USA

MANDIANT (5 yrs)

Microsoft (2 yrs)

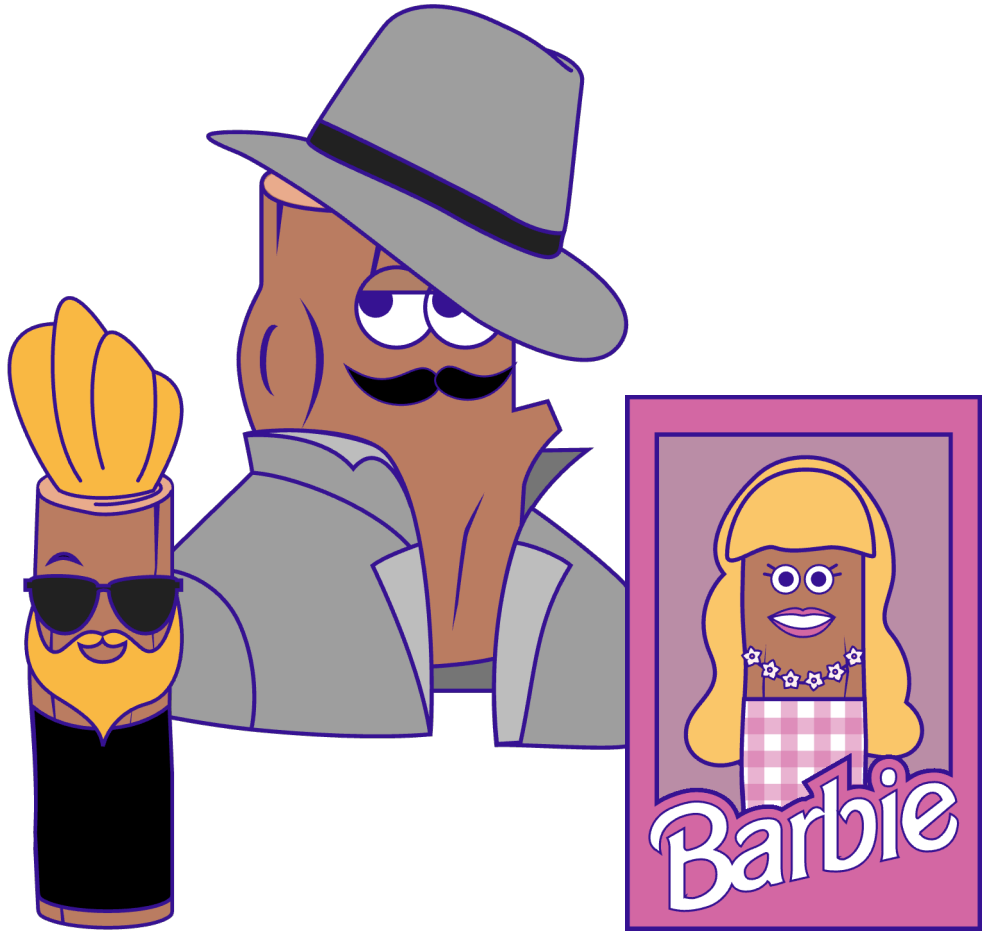
@danielhbohannon

danielhbohannon

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

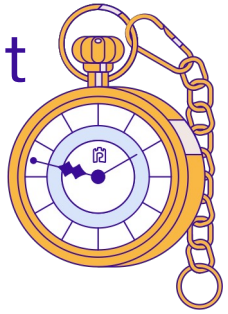


On-Prem vs Cloud Logs *(Data source, not storage location)*

- 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

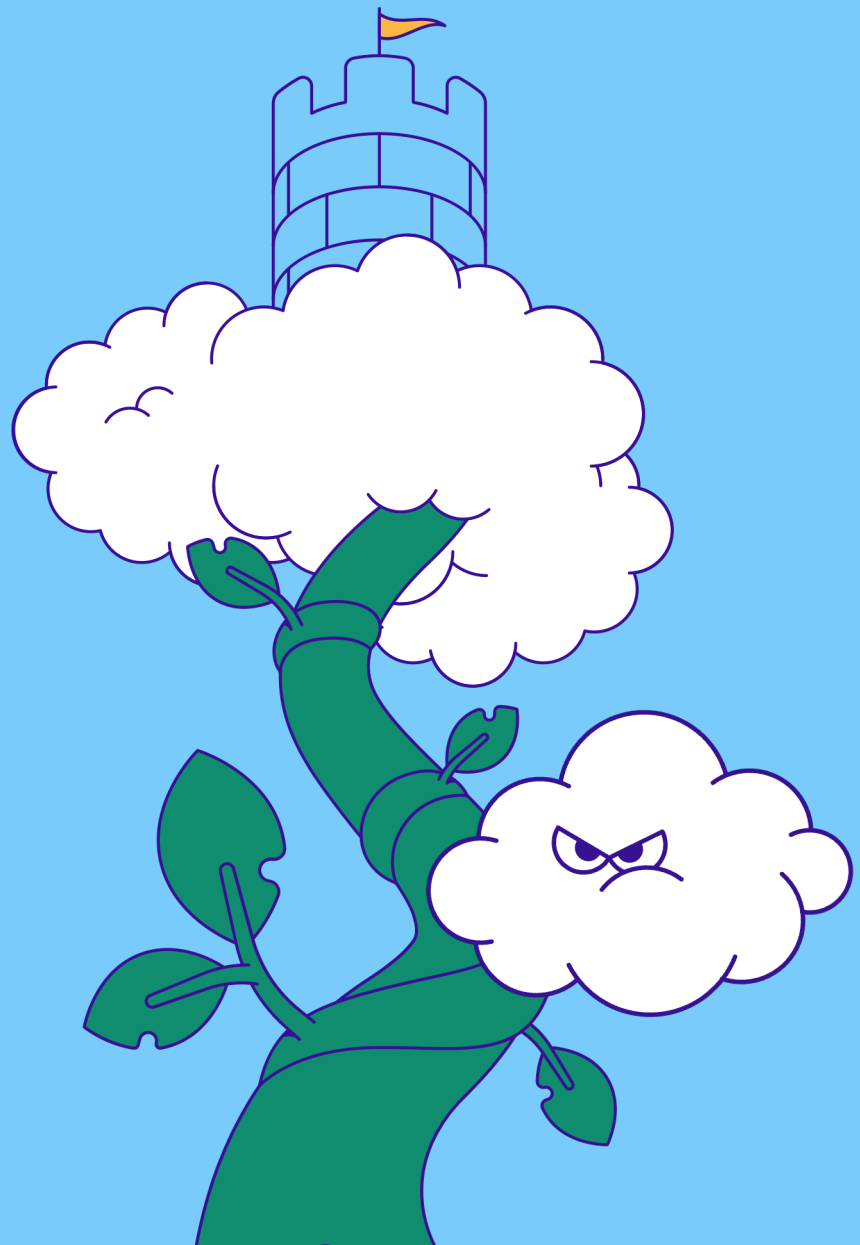
On-Prem vs Cloud Logs *(Data source, not storage location)*

- 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

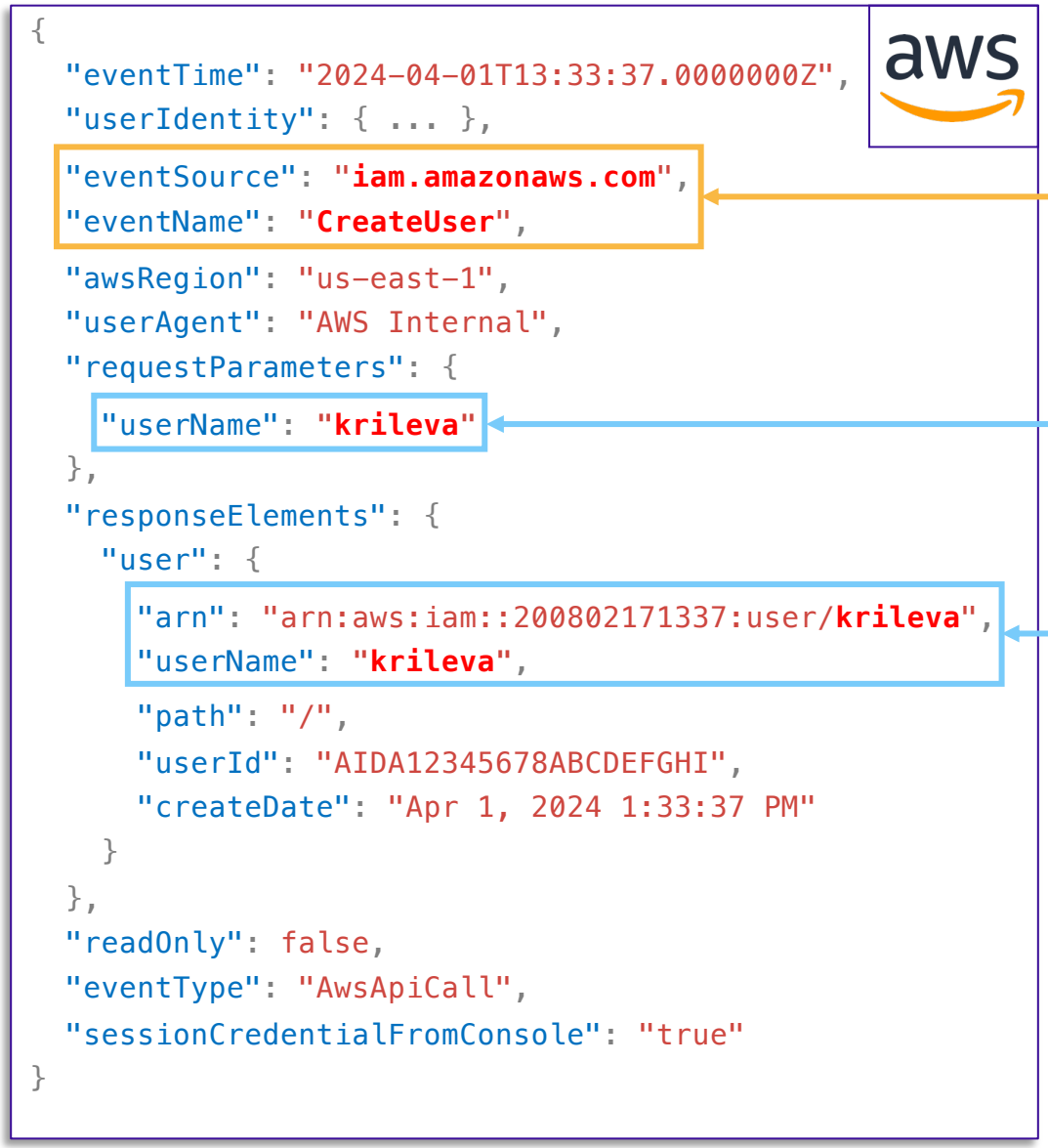


AGENDA

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



Cloud Log Examples – Creating a User

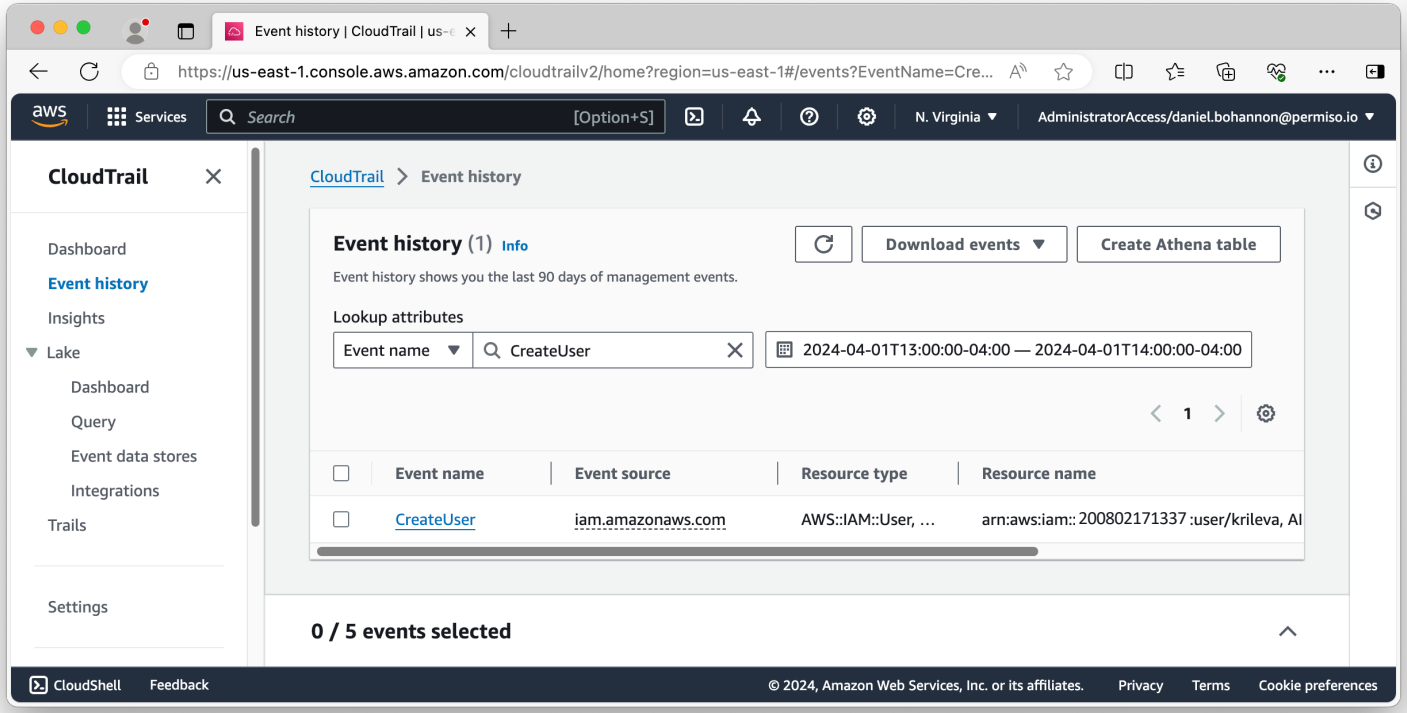


```
{
  "eventTime": "2024-04-01T13:33:37.0000000Z",
  "userIdentity": { ... },
  "eventSource": "iam.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "userName": "krileva"
  },
  "responseElements": {
    "user": {
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

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

Cloud Log Querying – API vs Forwarded

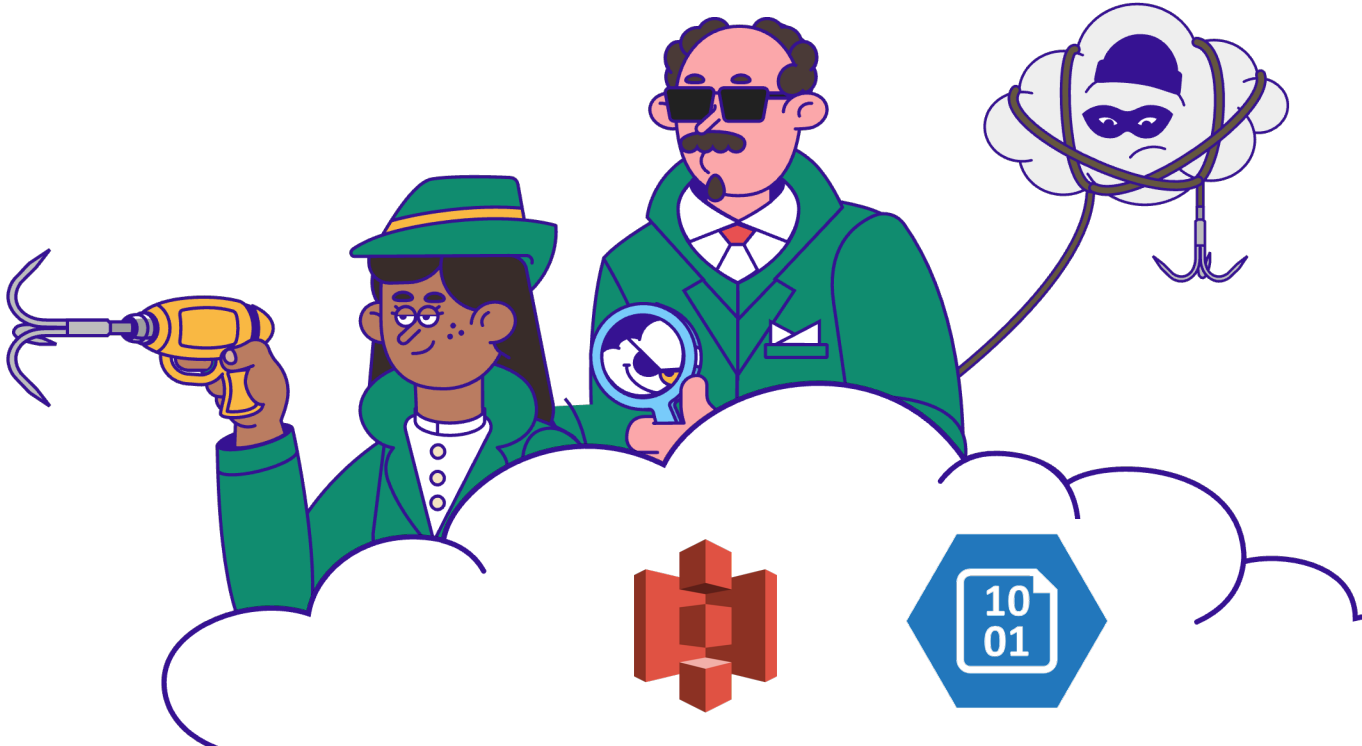
- API
  - PRO: Least delayed
  - CON: Limited retention
    (AWS = 90 days, Azure = 30 days)



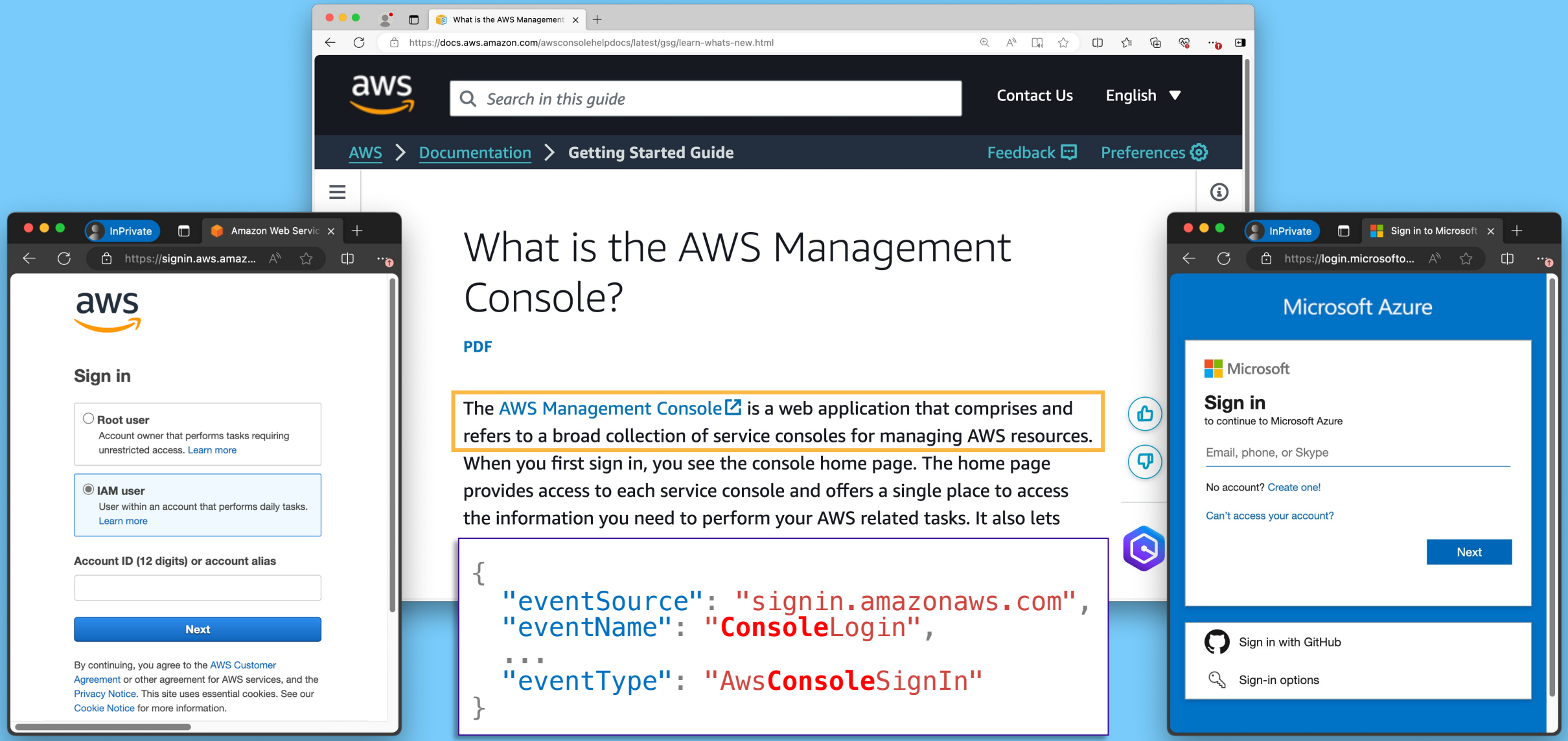

```
bash-3.2$
bash-3.2$ aws cloudtrail lookup-events \
>     --lookup-attributes AttributeKey=EventName,AttributeValue=CreateUser \
>     --start-time 2024-04-01T013:00:00 --end-time 2024-04-01T14:00:00
{
    "Events": [
        {
            "EventId": "db014773-abcd-1234-5678-133337c0ffee",
      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

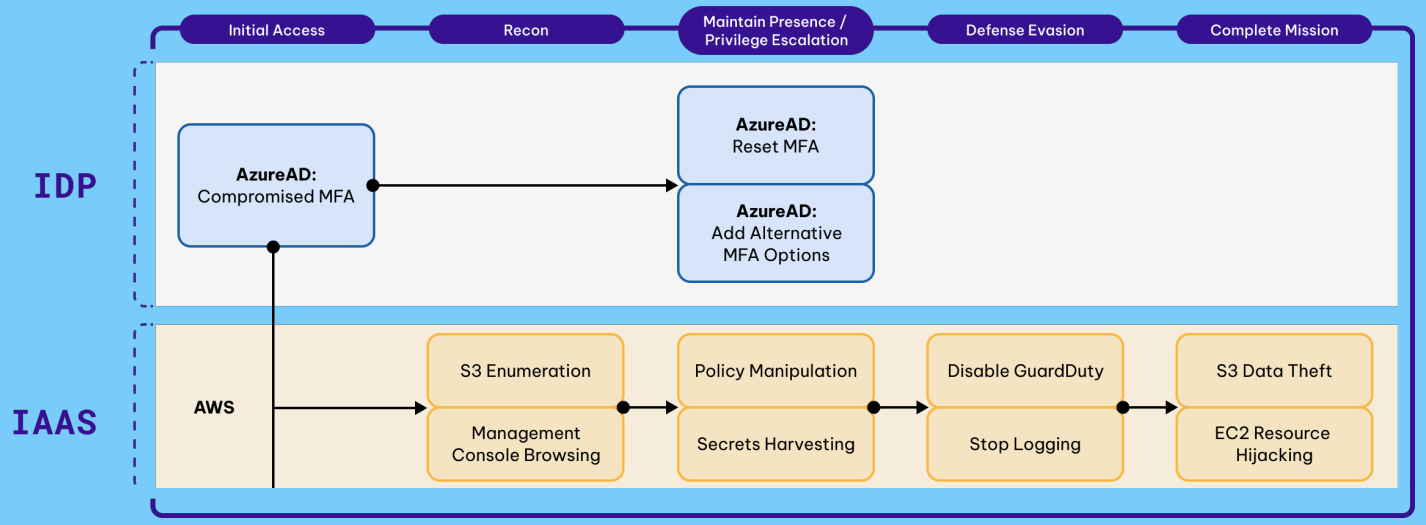


Definition: Console



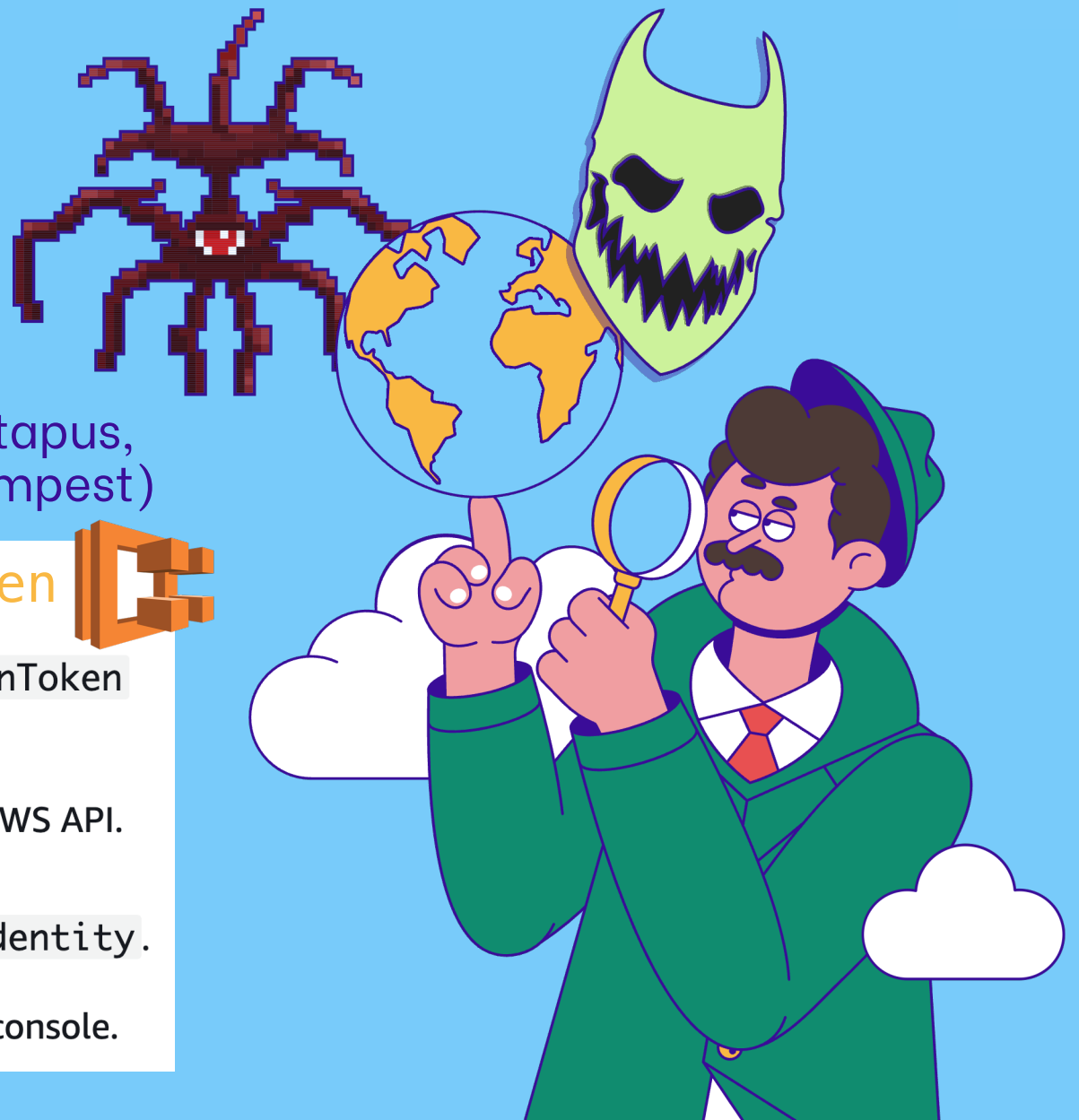
Console Usage in the Wild

- Threat actors
  - LUCR-1
    - aka GUI-vil
  - LUCR-3
    - aka Scattered Spider, Roasted 0ktapus, UNC3944, STORM-0875 (Octo Tempest)



Console Usage in the Wild

- Threat actors
  - LUCR-1
    - aka GUI-vil
  - LUCR-3
    - aka Scattered Spider, Roasted 0ktapus, UNC3944, STORM-0875 (Octo Tempest)



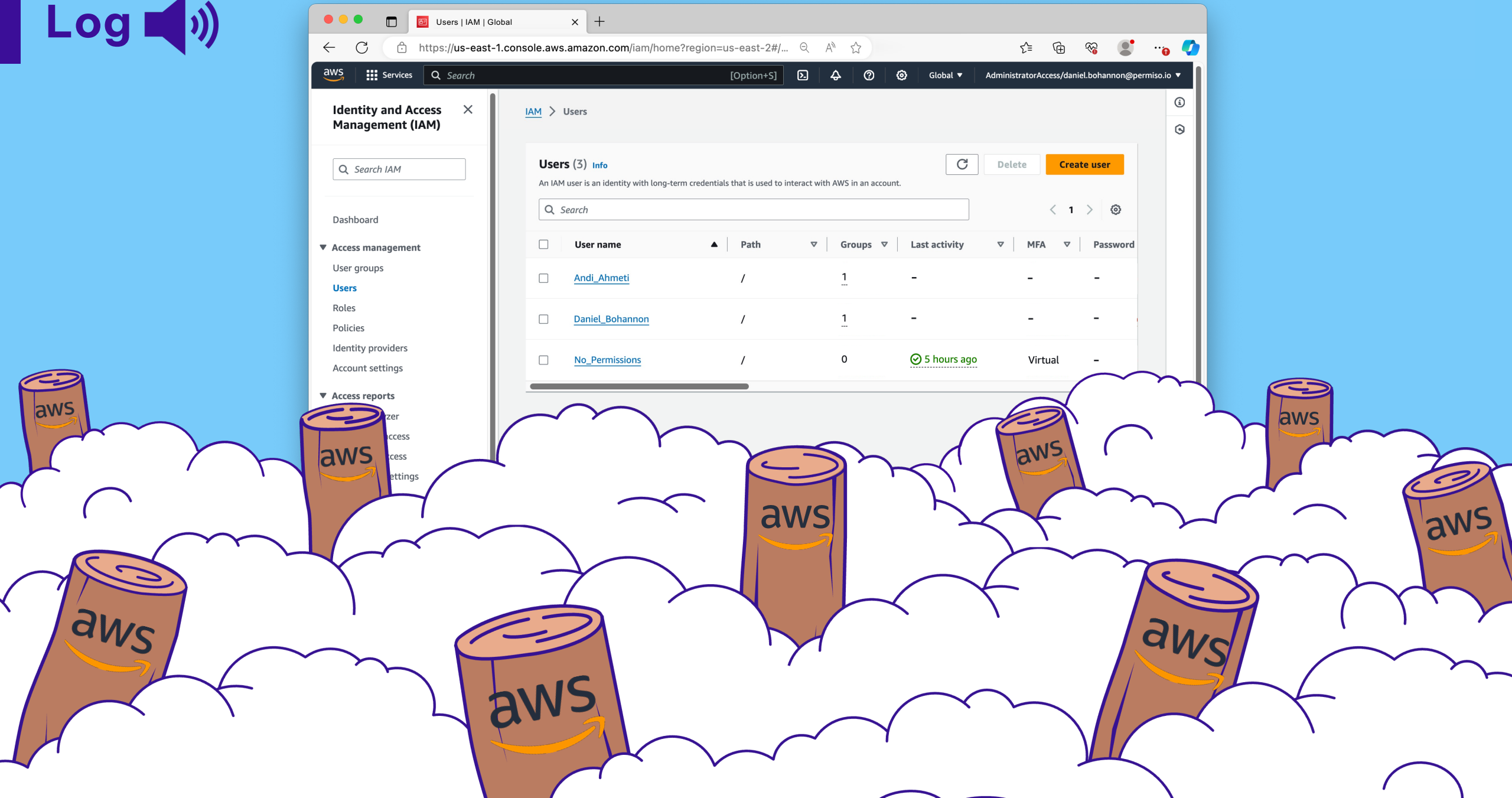
Permissions `sts:GetFederationToken`

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

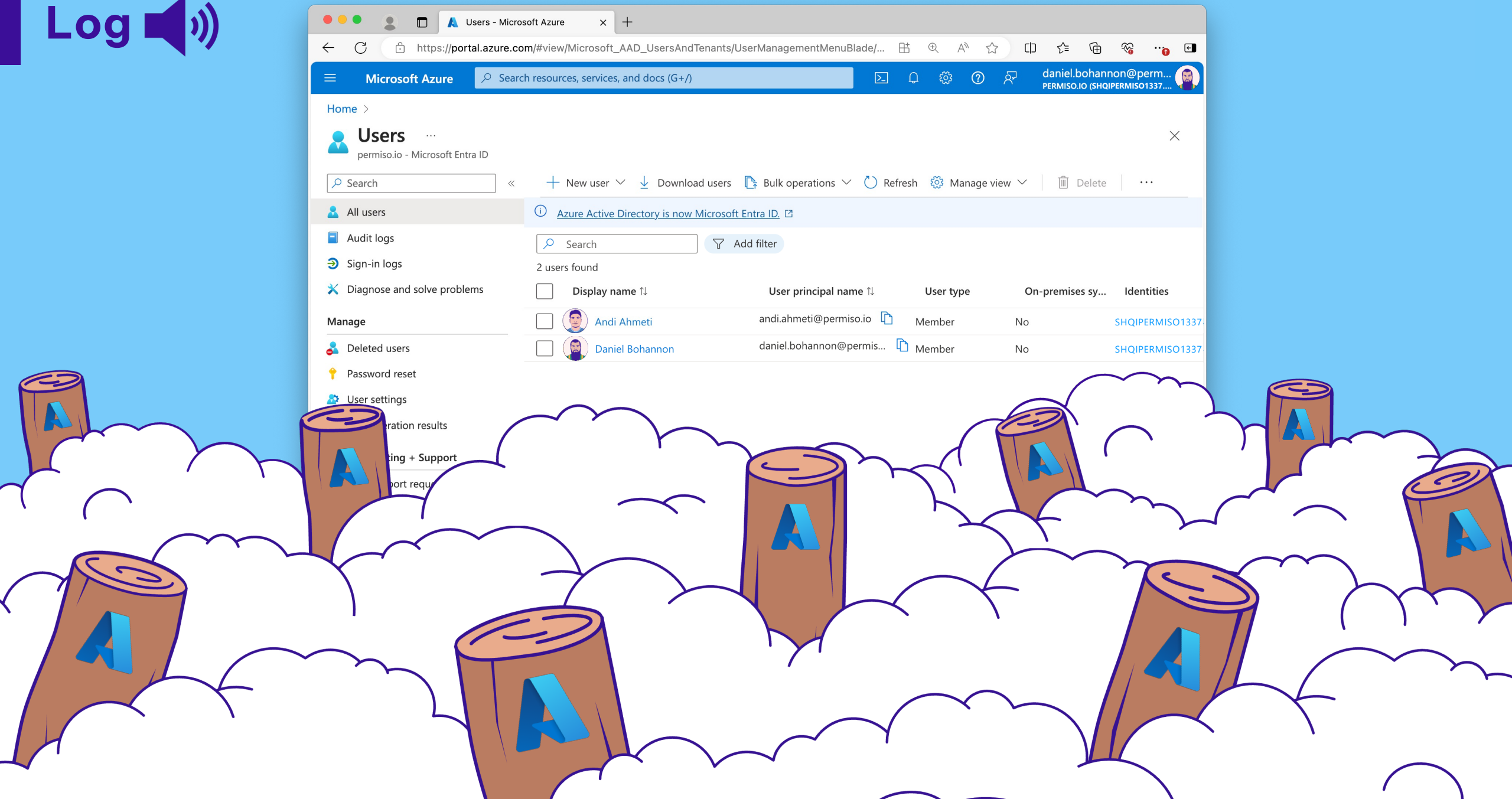
- You cannot call any IAM operations using the AWS CLI or the AWS API. This limitation does not apply to console sessions.
- You cannot call any AWS STS operations except `GetCallerIdentity`.

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

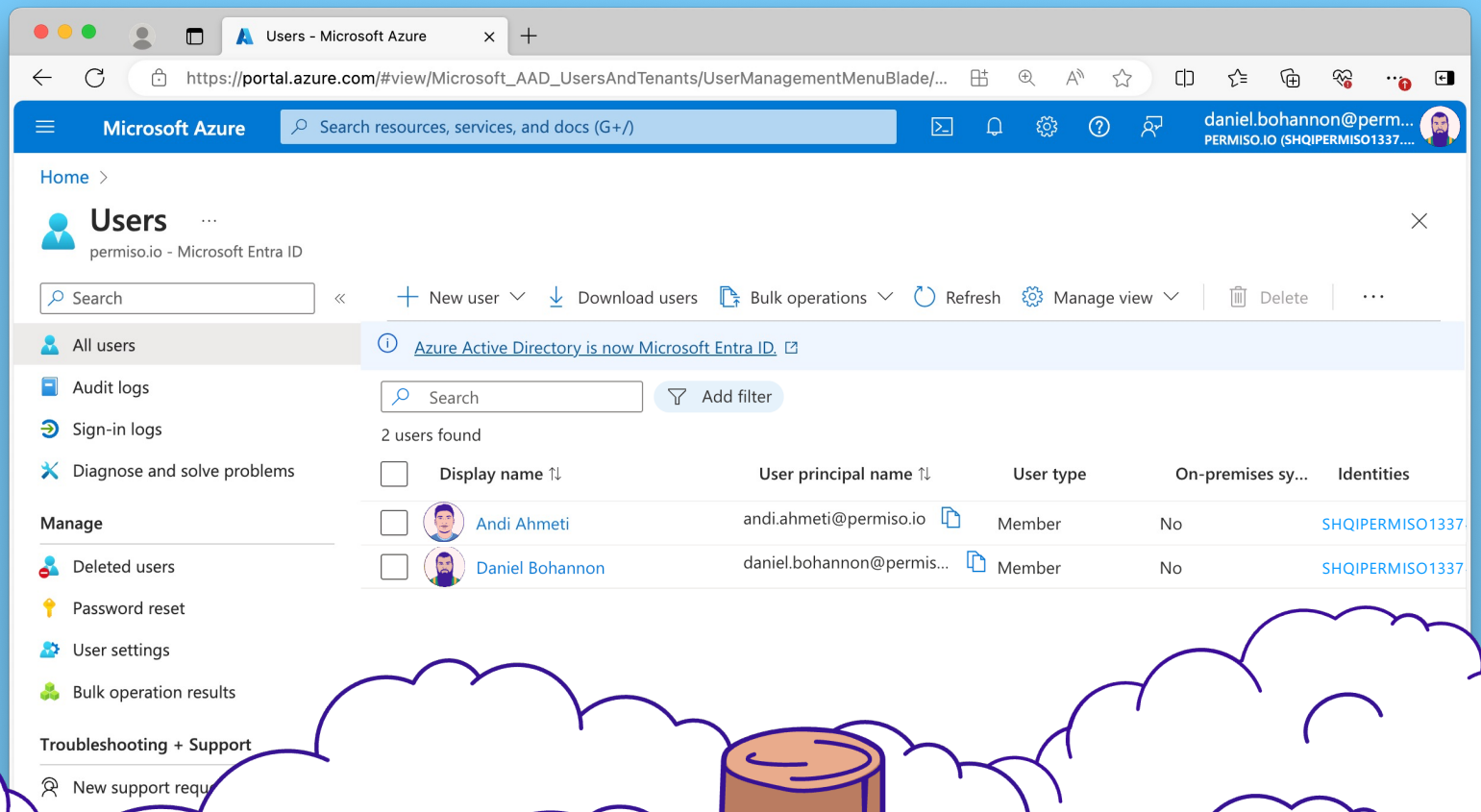
Log


Users | IAM | Global
https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/...
aws
Services
Search
[Option+S]
Global
AdministratorAccess/daniel.bohannon@permiso.io
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
IAM > Users
Users (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
1
User name
Path
Groups
Last activity
MFA
Password
Andi_Ahmeti
/
1
-
-
-
Daniel_Bohannon
/
1
-
-
-
No_Permissions
/
0
5 hours ago
Virtual
-

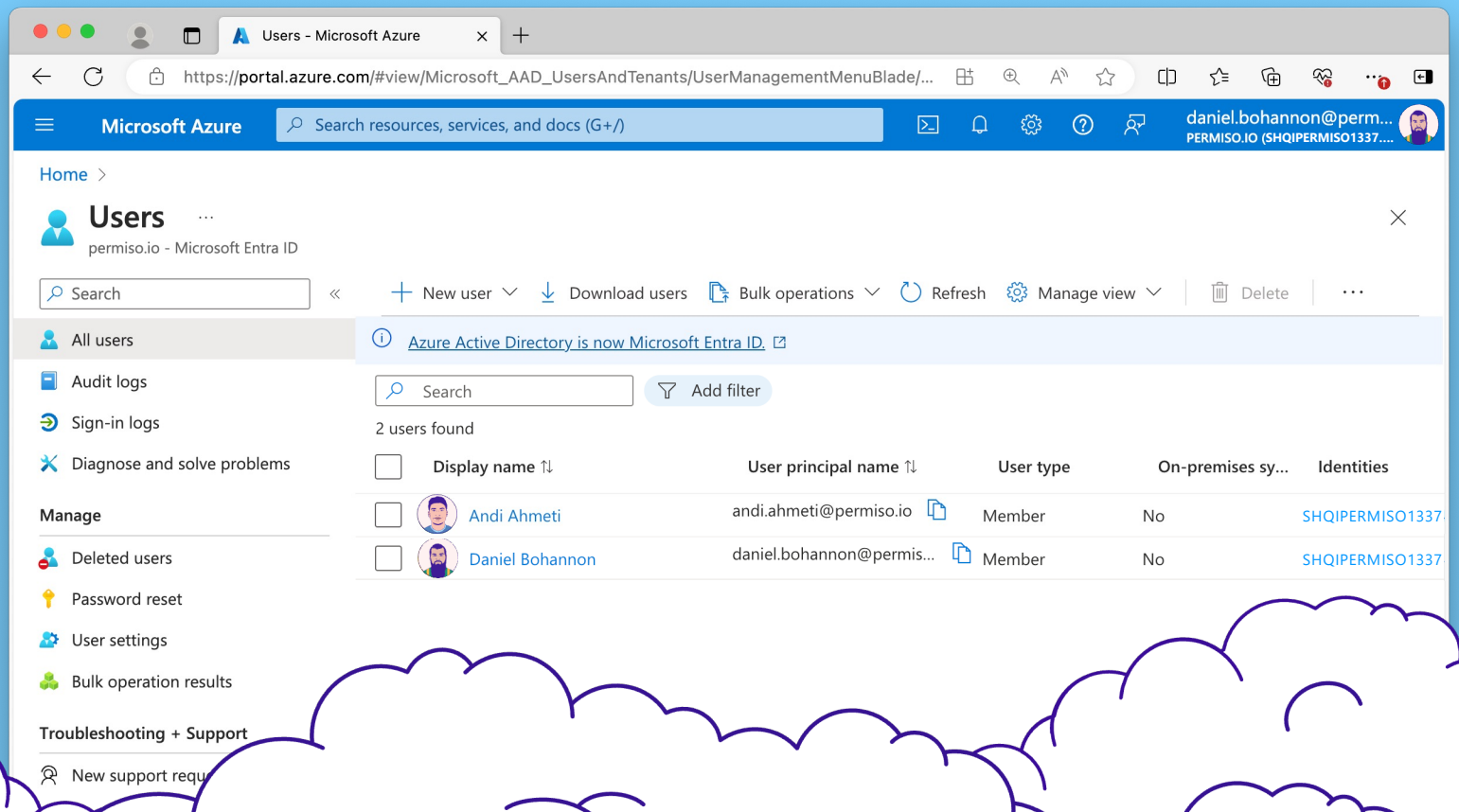
Log


Users - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/...
Microsoft Azure
Search resources, services, and docs (G+/)
daniel.bohannon@perm...
PERMISO.IO (SHQIPERMISO1337....
Home
Users
permiso.io - Microsoft Entra ID
Search
New user
Download users
Bulk operations
Refresh
Manage view
Delete
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Deleted users
Password reset
User settings
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter
2 users found
Display name
User principal name
User type
On-premises sy...
Identities
Andi Ahmeti
andi.ahmeti@permiso.io
Member
No
SHQIPERMISO1337
Daniel Bohannon
daniel.bohannon@permis...
Member
No
SHQIPERMISO1337

Log


Users - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/...
Microsoft Azure
Search resources, services, and docs (G+/)
daniel.bohannon@perm...
PERMISO.IO (SHQIPERMISO1337....
Home
Users
permiso.io - Microsoft Entra ID
Search
New user
Download users
Bulk operations
Refresh
Manage view
Delete
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Deleted users
Password reset
User settings
Bulk operation results
Troubleshooting + Support
New support requ
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter
2 users found
Display name
User principal name
User type
On-premises sy...
Identities
Andi Ahmeti
andi.ahmeti@permiso.io
Member
No
SHQIPERMISO1337
Daniel Bohannon
daniel.bohannon@permis...
Member
No
SHQIPERMISO1337

Log

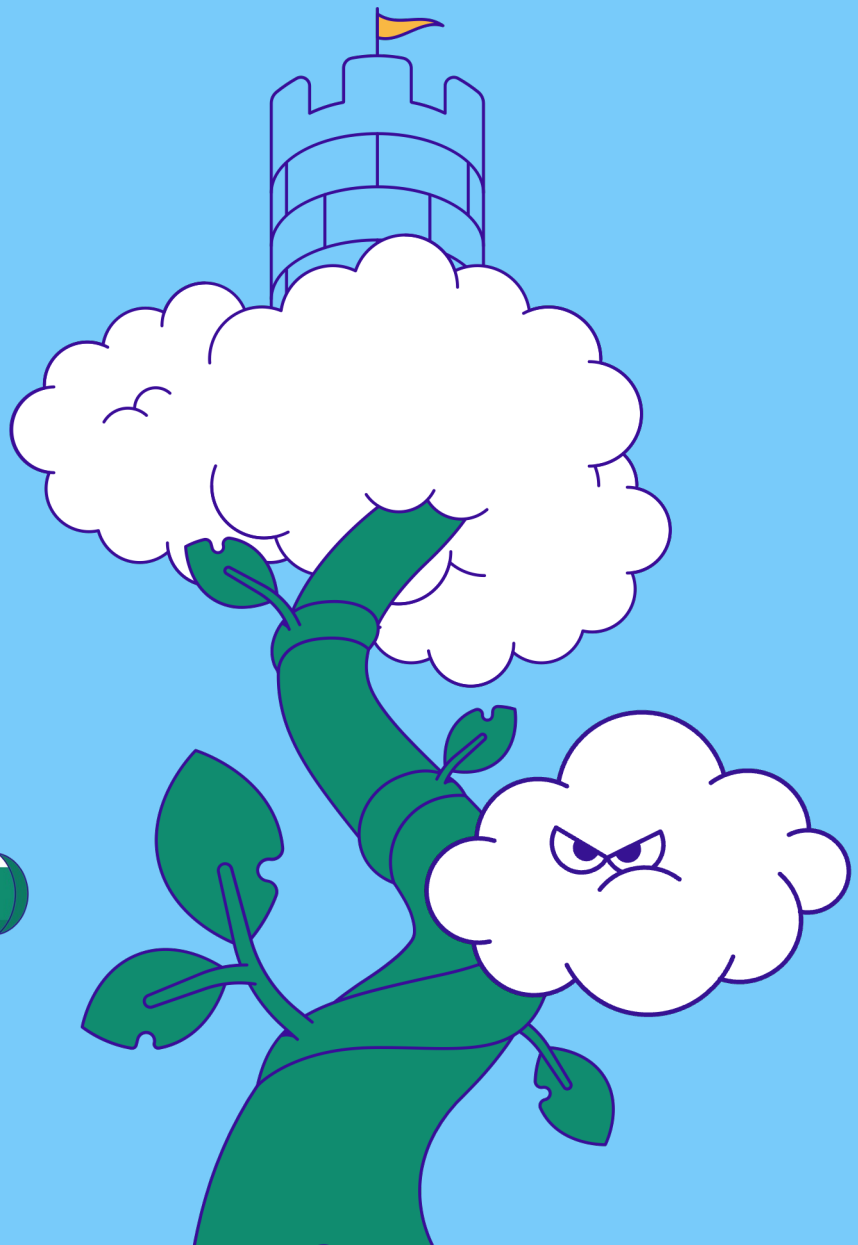

Users - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/...
Microsoft Azure
Search resources, services, and docs (G+/)
daniel.bohannon@perm...
PERMISO.IO (SHQIPERMISO1337....
Home
Users
permiso.io - Microsoft Entra ID
Search
New user
Download users
Bulk operations
Refresh
Manage view
Delete
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Deleted users
Password reset
User settings
Bulk operation results
Troubleshooting + Support
New support requ
Azure Active Directory is now Microsoft Entra ID.
Search
Add filter
2 users found
Display name
User principal name
User type
On-premises sy...
Identities
Andi Ahmeti
andi.ahmeti@permiso.io
Member
No
SHQIPERMISO1337
Daniel Bohannon
daniel.bohannon@permis...
Member
No
SHQIPERMISO1337


NO, N-NOT YOU,
Azure


aws

AGENDA

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

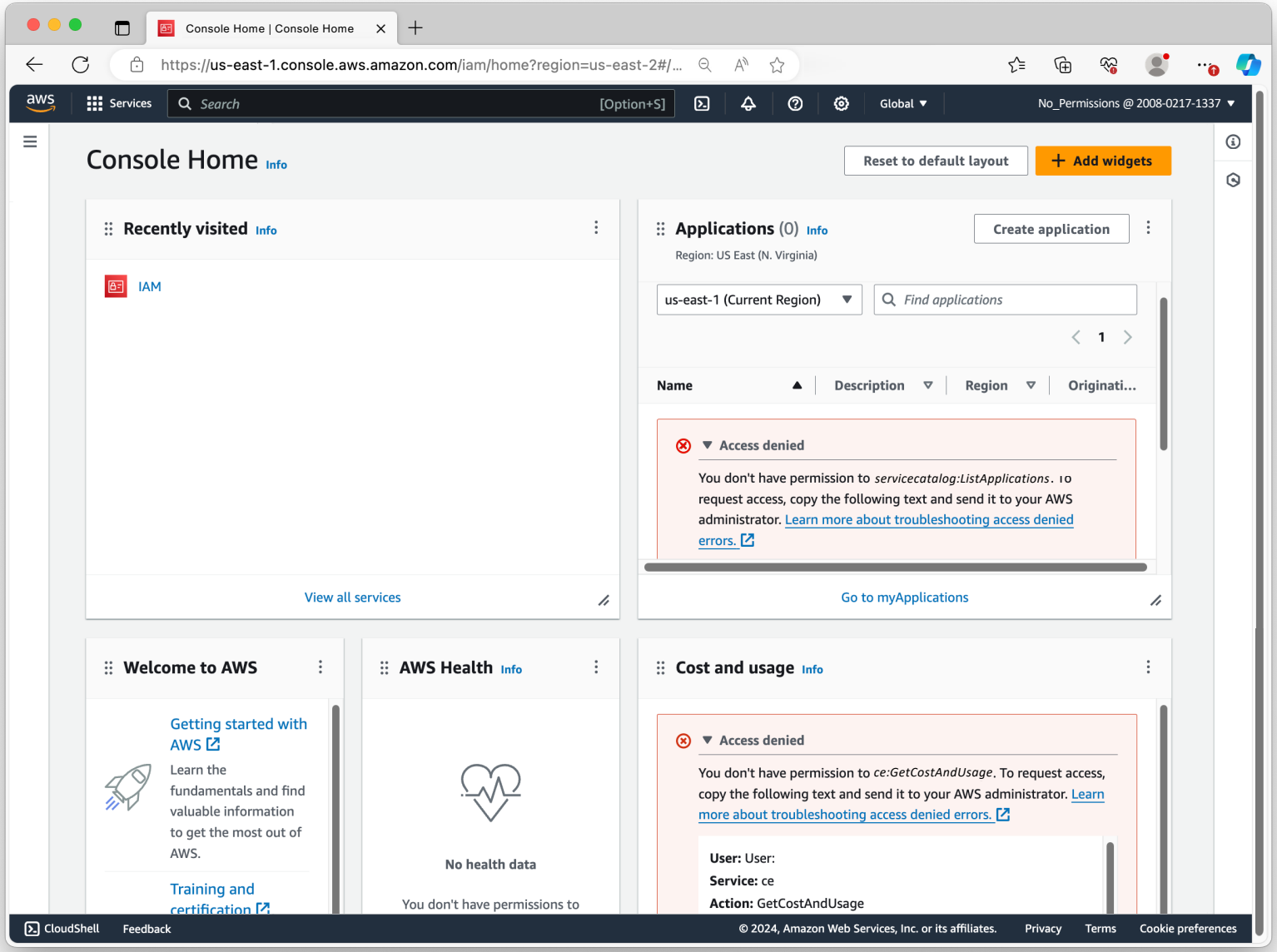


AGENDA

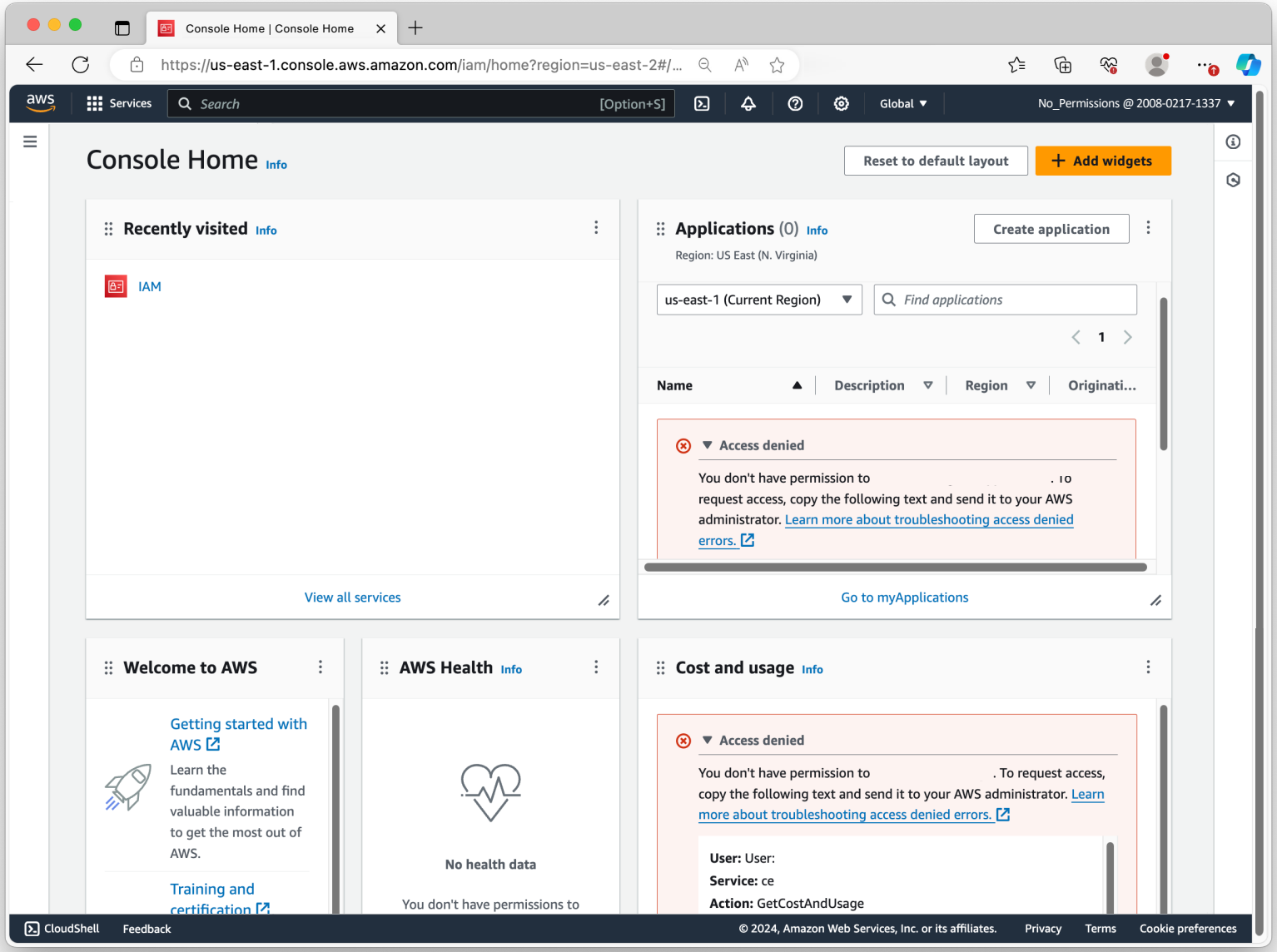
- **PROBLEM: Noisy Console Logs** 👀


033 5 1

No Permissions – 1/3 – Console Home



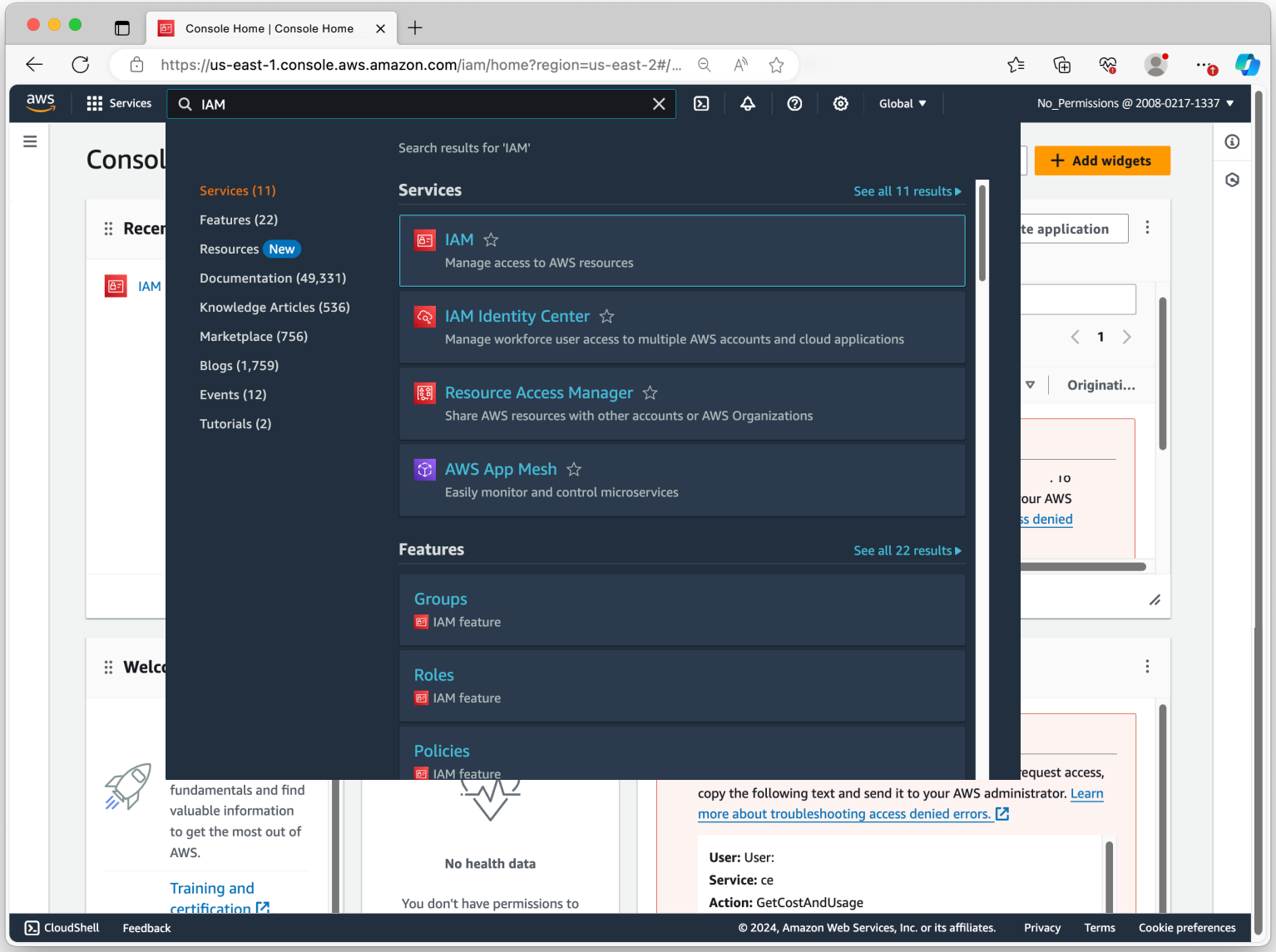
No Permissions – 1/3 – Console Home



servicecatalog:ListApplications

ce:GetCostAndUsage

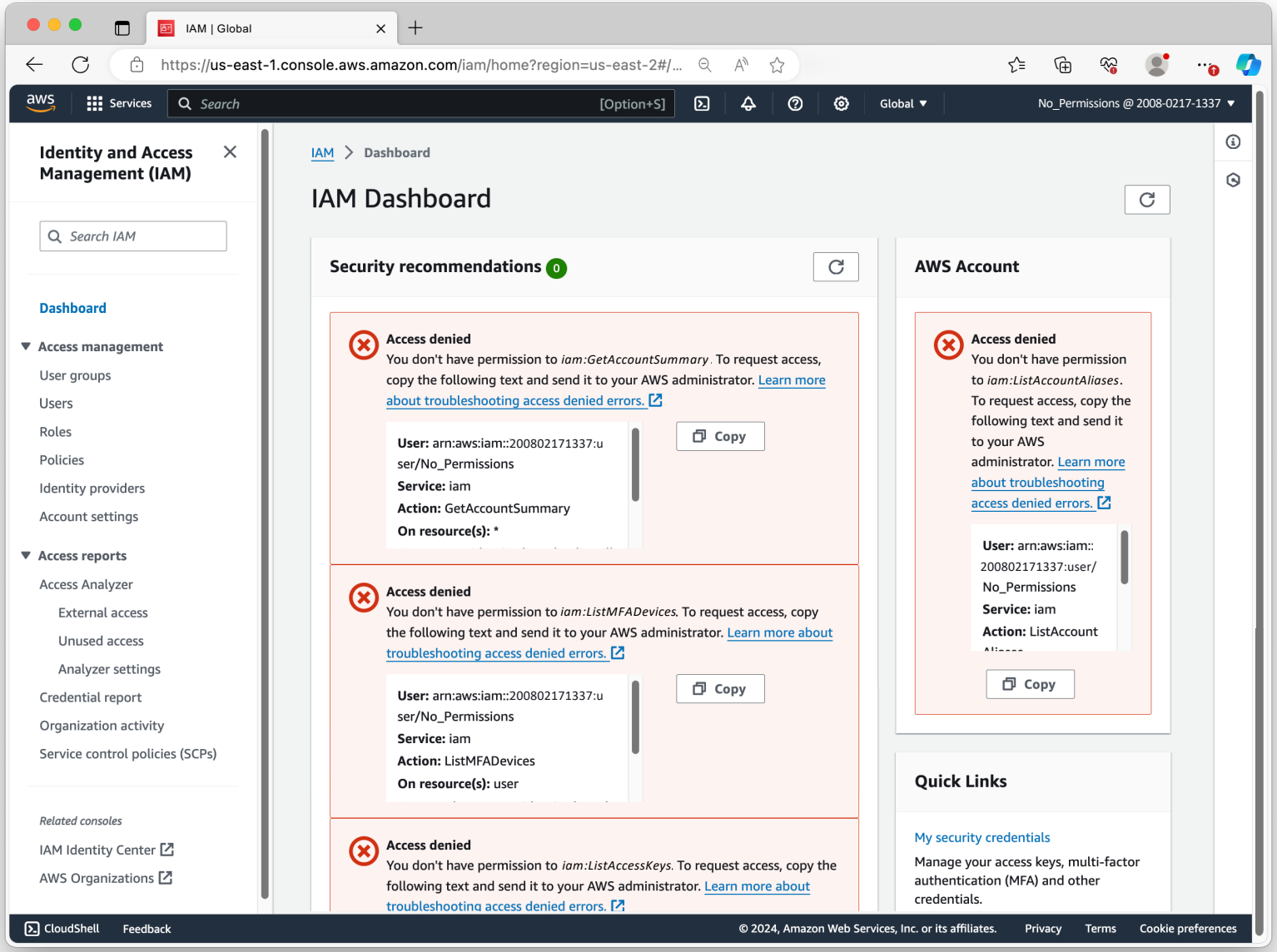
No Permissions – 1/3 – Console Home



servicecatalog:ListApplications

ce:GetCostAndUsage

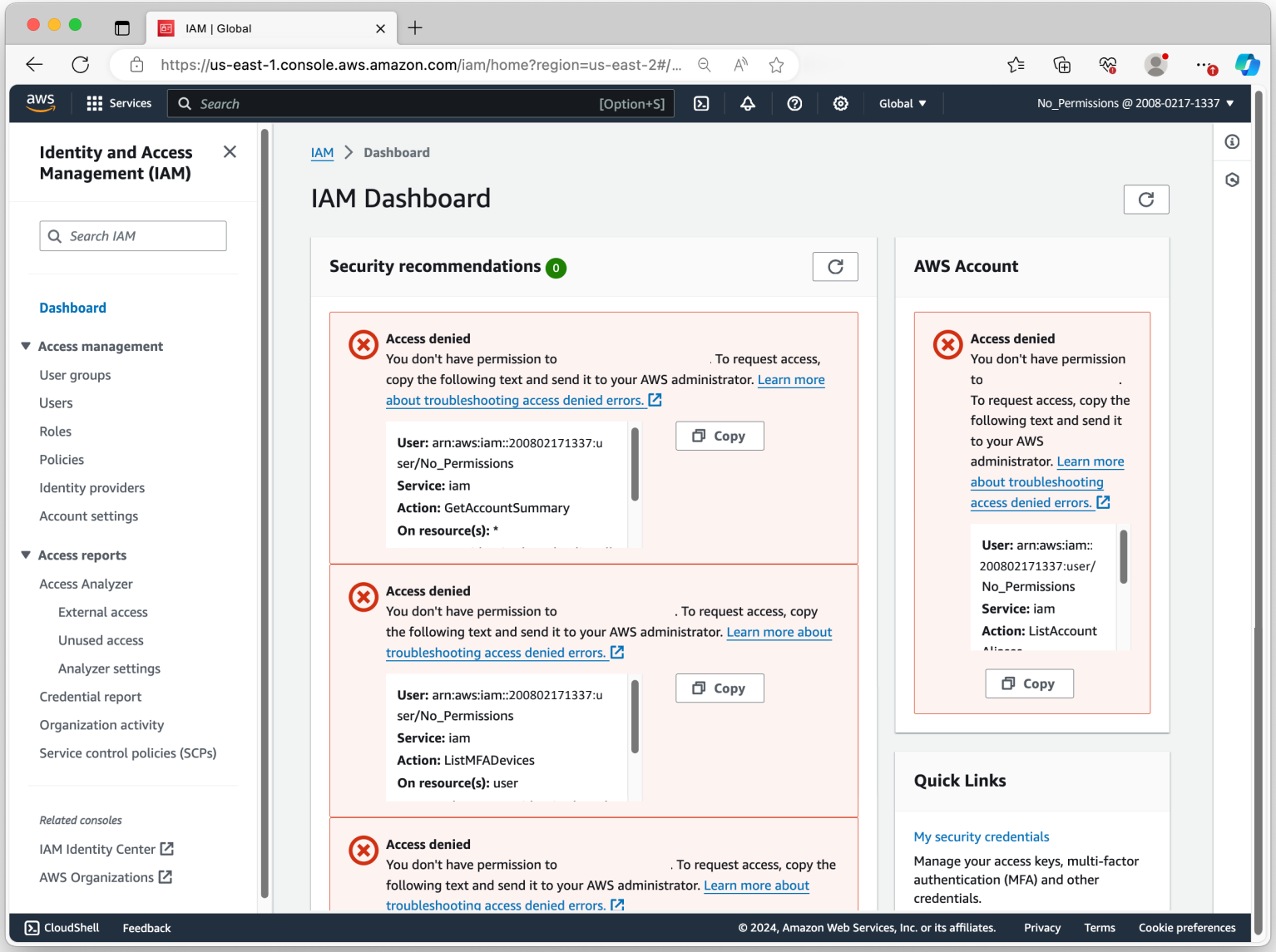
No Permissions – 2/3 – IAM Dashboard



servicecatalog:ListApplications

ce:GetCostAndUsage

No Permissions – 2/3 – IAM Dashboard



servicecatalog:ListApplications

ce:GetCostAndUsage

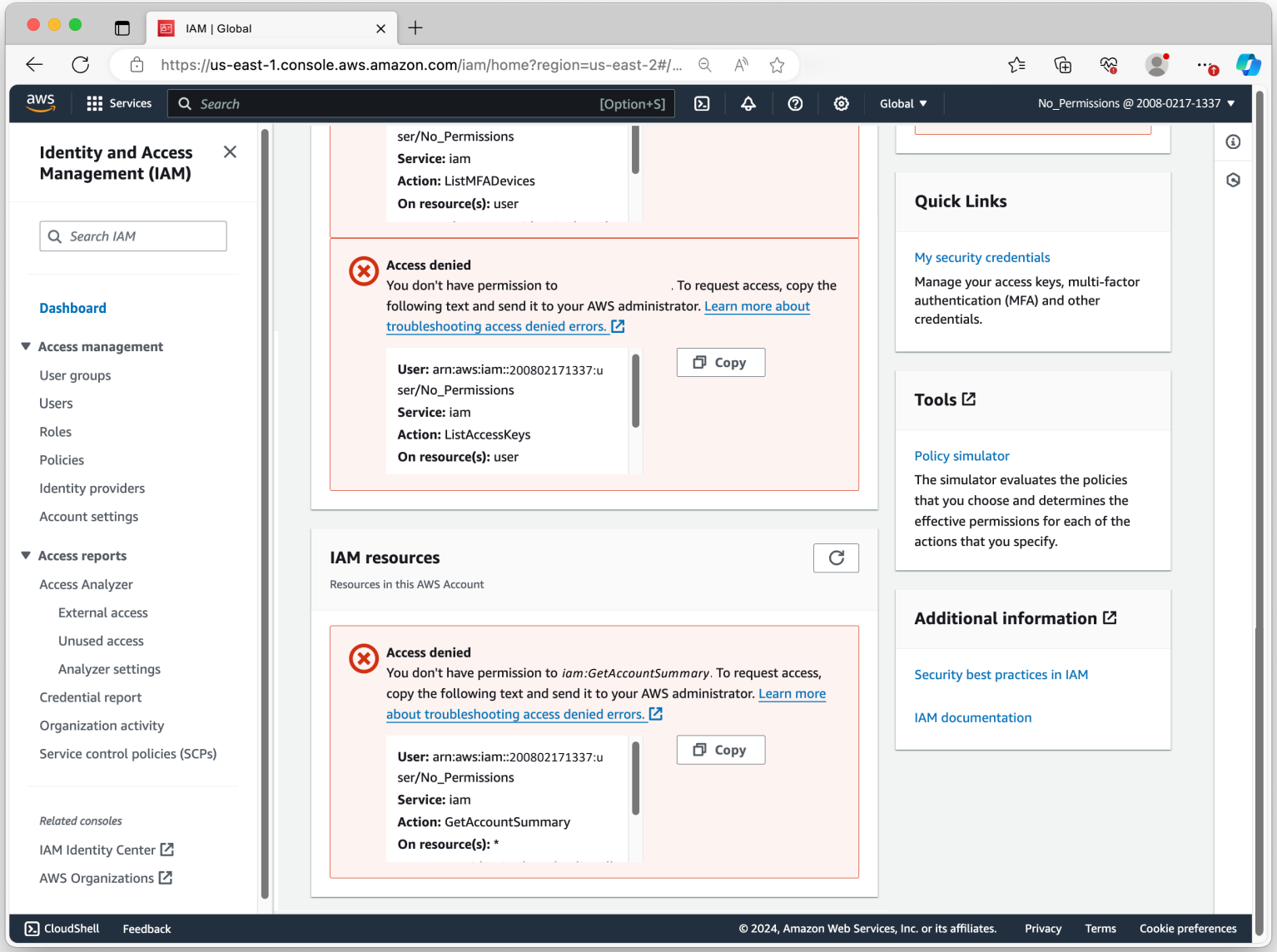
iam:ListAccountAliases

iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

No Permissions – 2/3 – IAM Dashboard



servicecatalog:ListApplications

ce:GetCostAndUsage

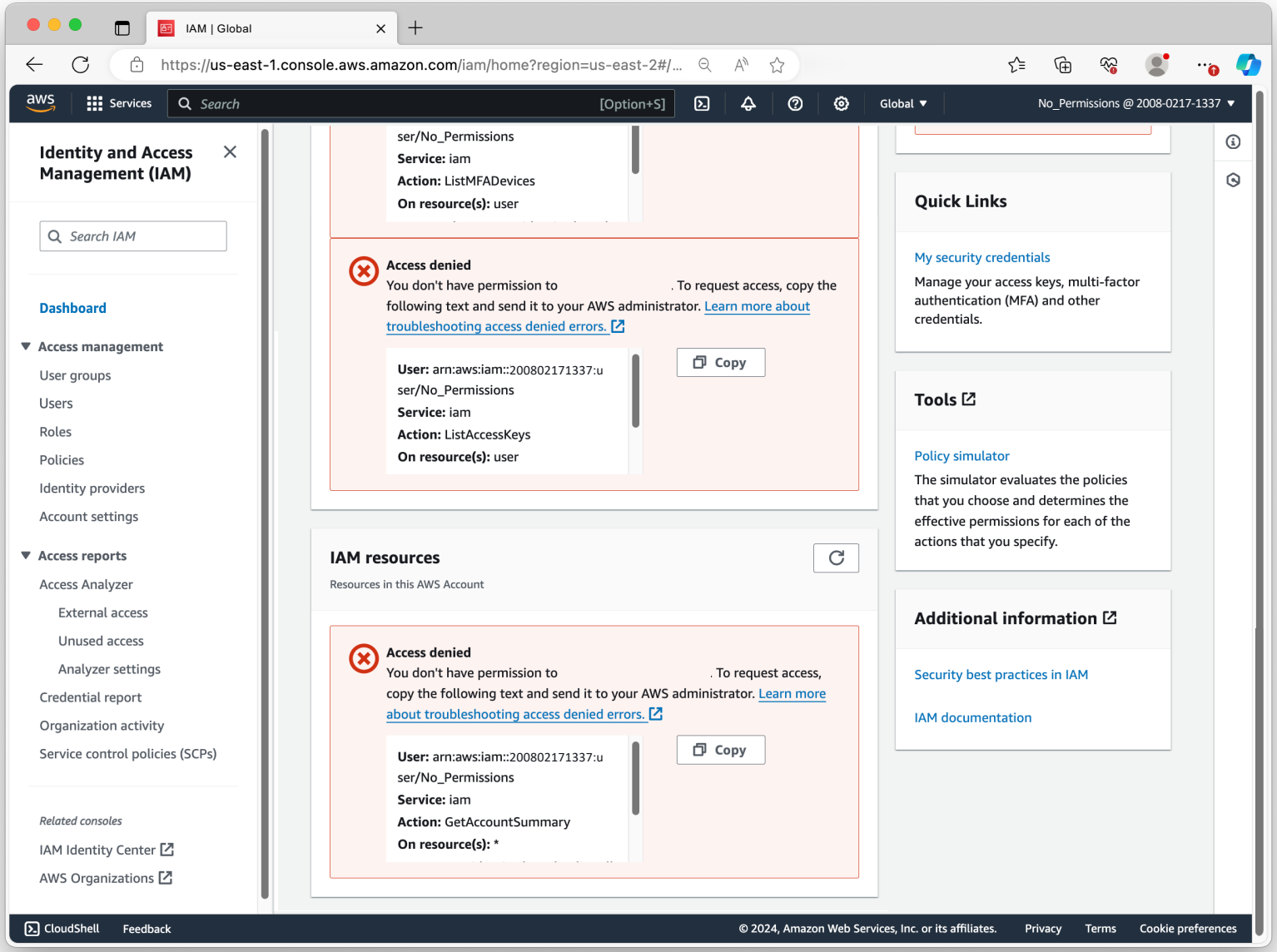
iam:ListAccountAliases

iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

No Permissions – 2/3 – IAM Dashboard



servicecatalog:ListApplications

ce:GetCostAndUsage

iam:ListAccountAliases

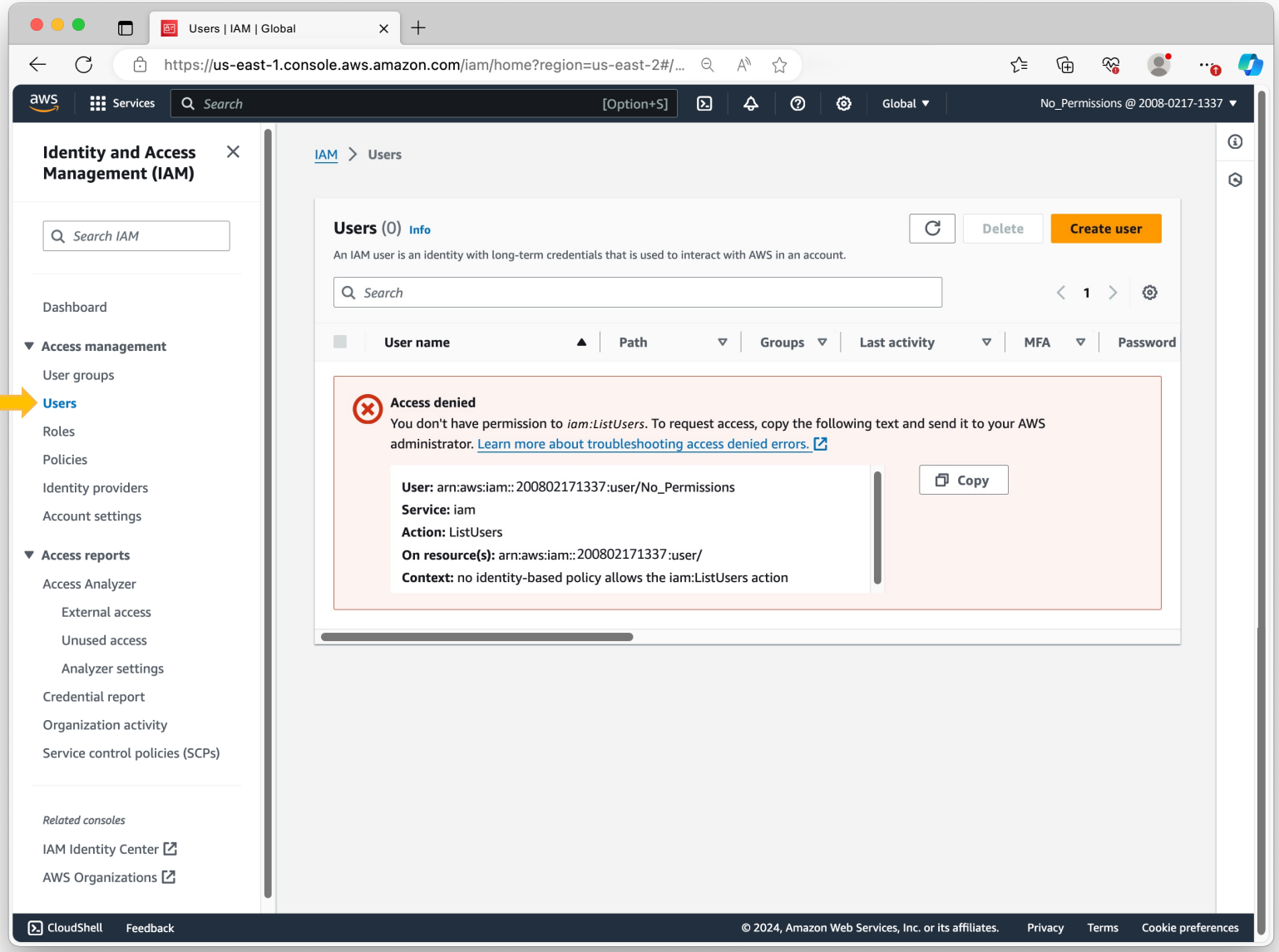
iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

iam:GetAccountSummary

No Permissions – 3/3 – IAM Users



servicecatalog:ListApplications

ce:GetCostAndUsage

iam:ListAccountAliases

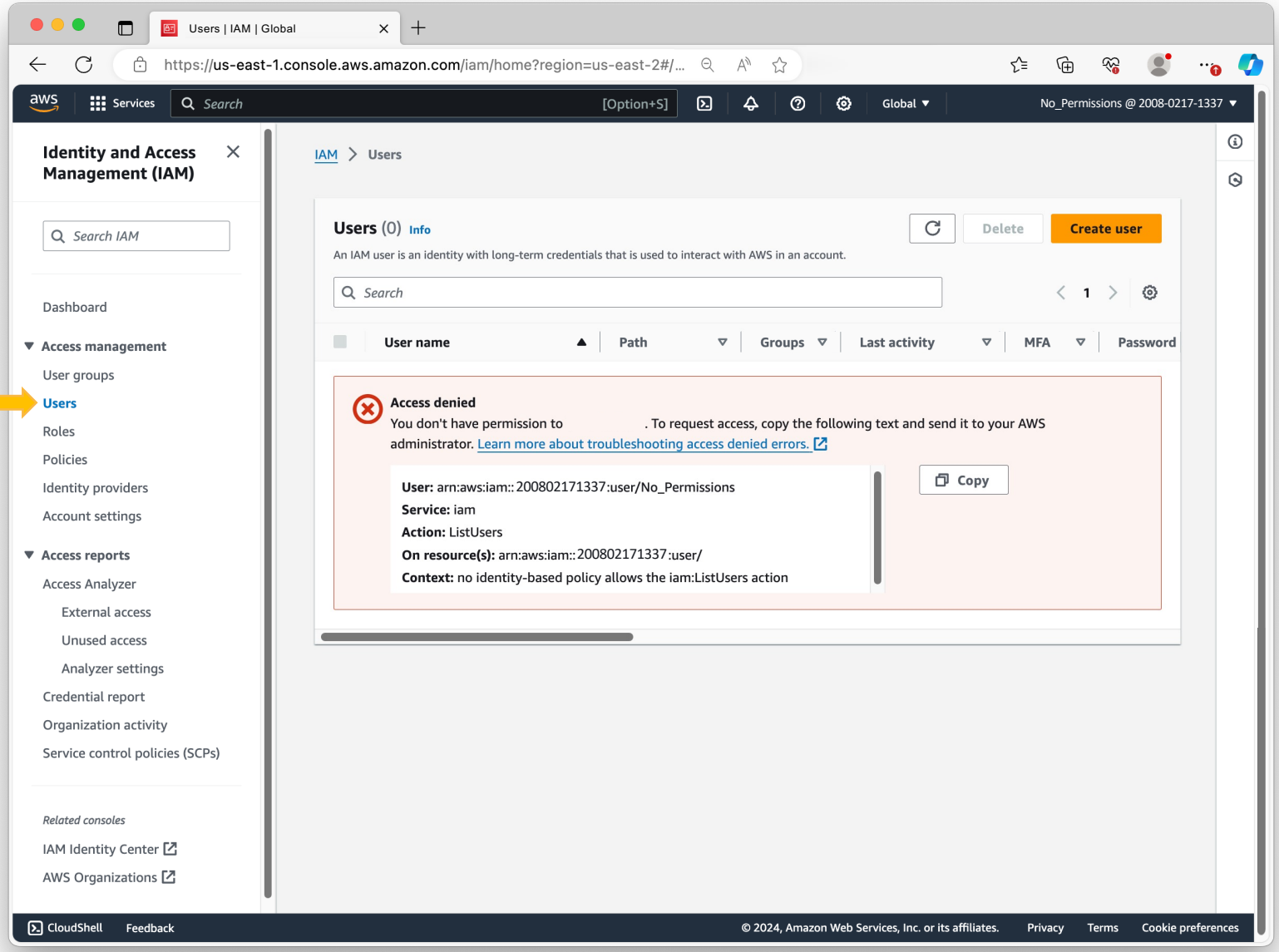
iam:GetAccountSummary

iam:ListMFADevices

iam:ListAccessKeys

iam:GetAccountSummary

No Permissions – 3/3 – IAM Users



servicecatalog:ListApplications

ce:GetCostAndUsage

iam:ListAccountAliases

iam:GetAccountSummary

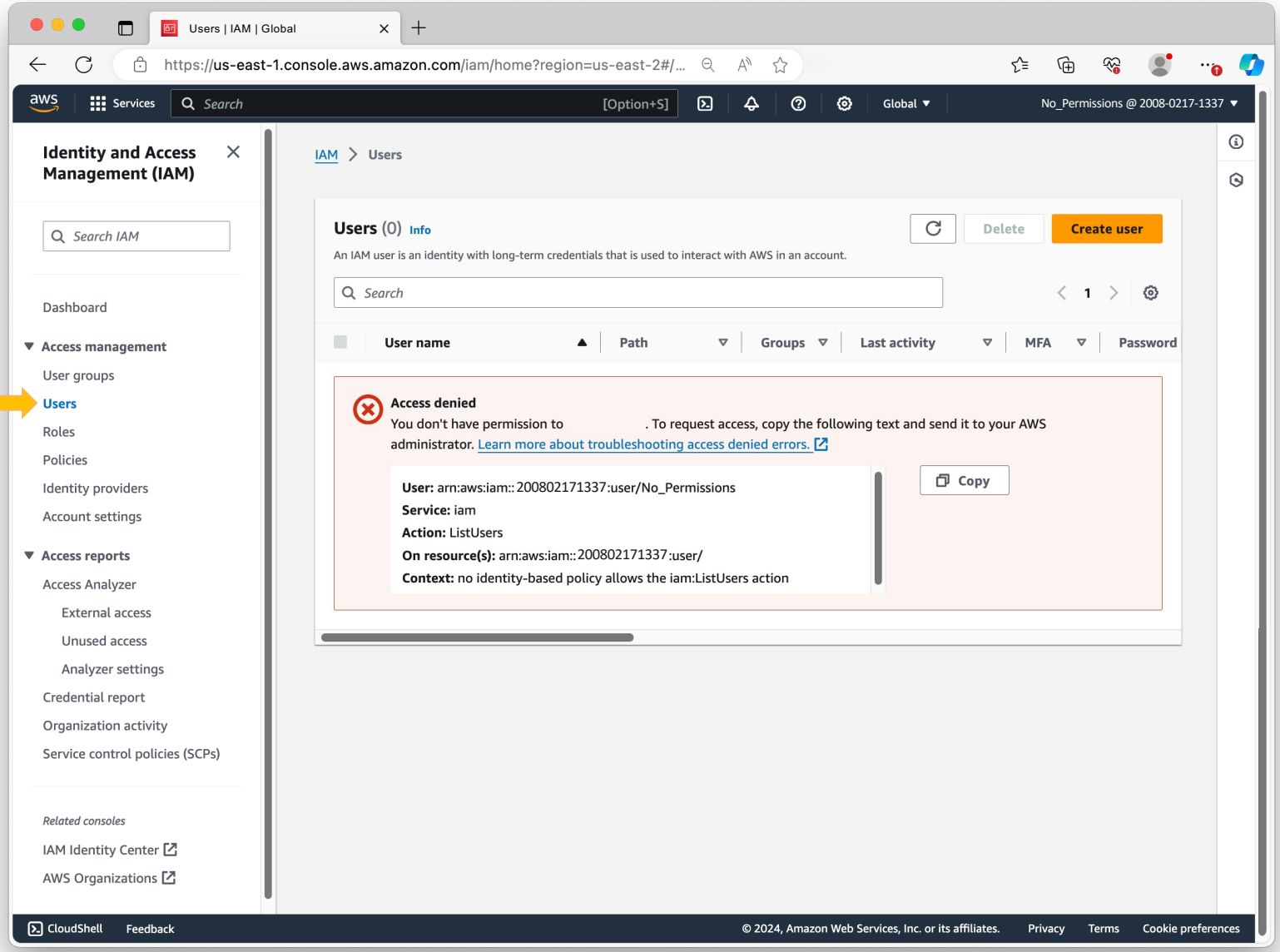
iam:ListMFADevices

iam:ListAccessKeys

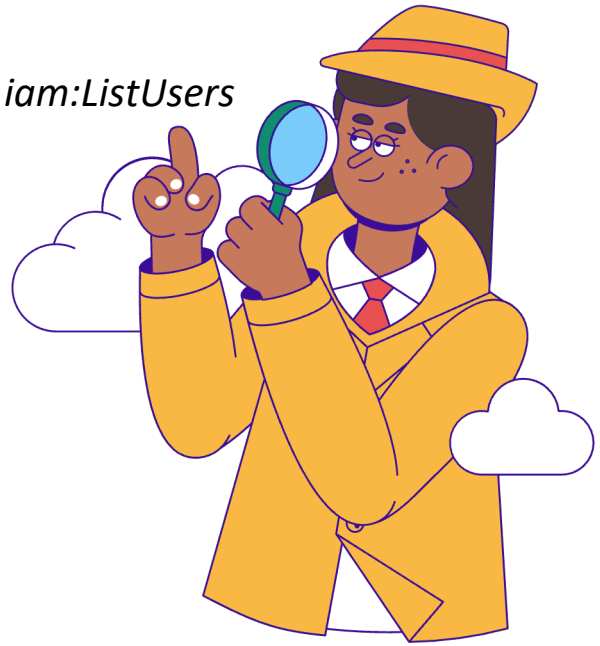
iam:GetAccountSummary

iam:ListUsers

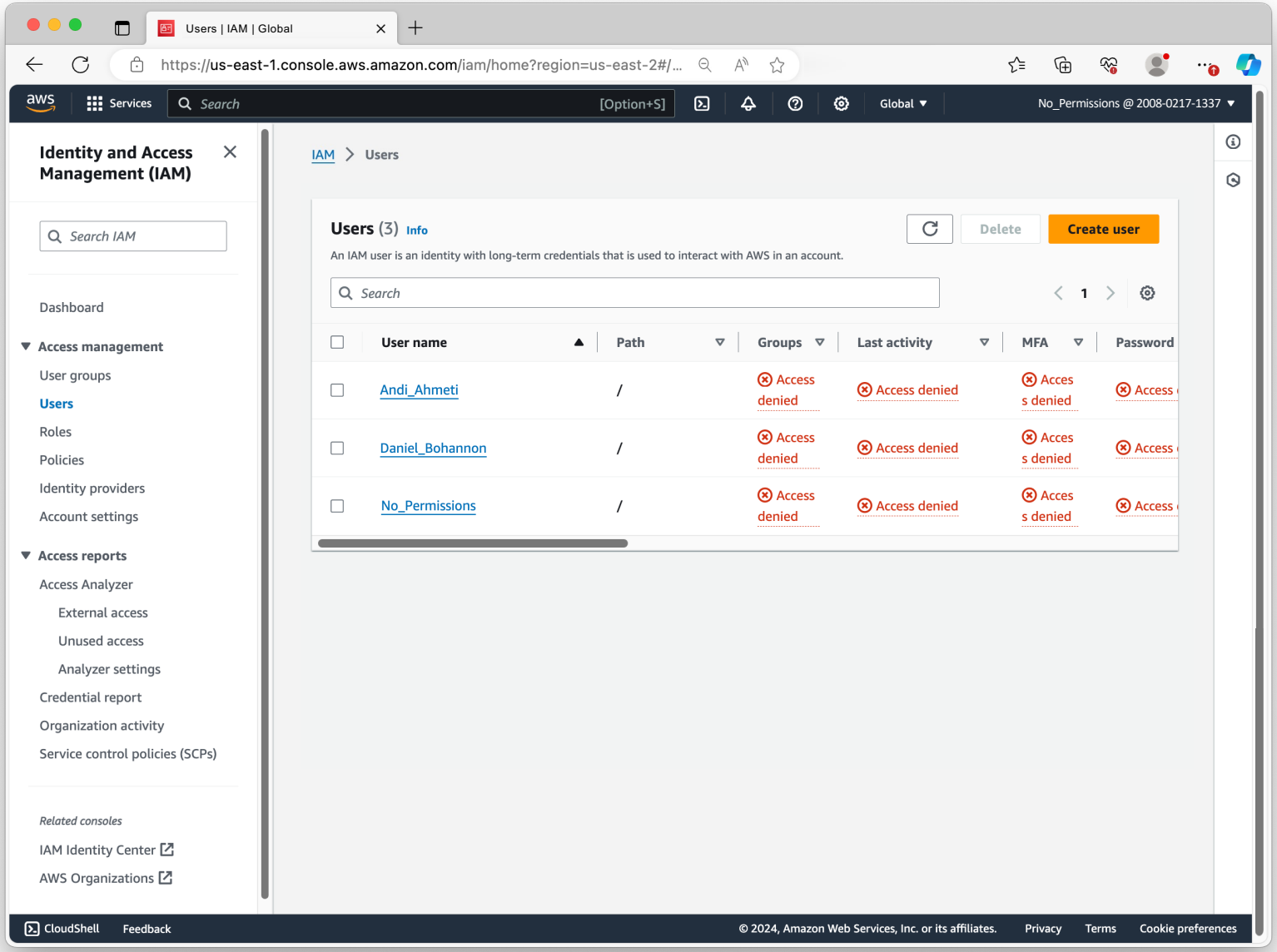
No Permissions – 3/3 – IAM Users



iam:ListUsers

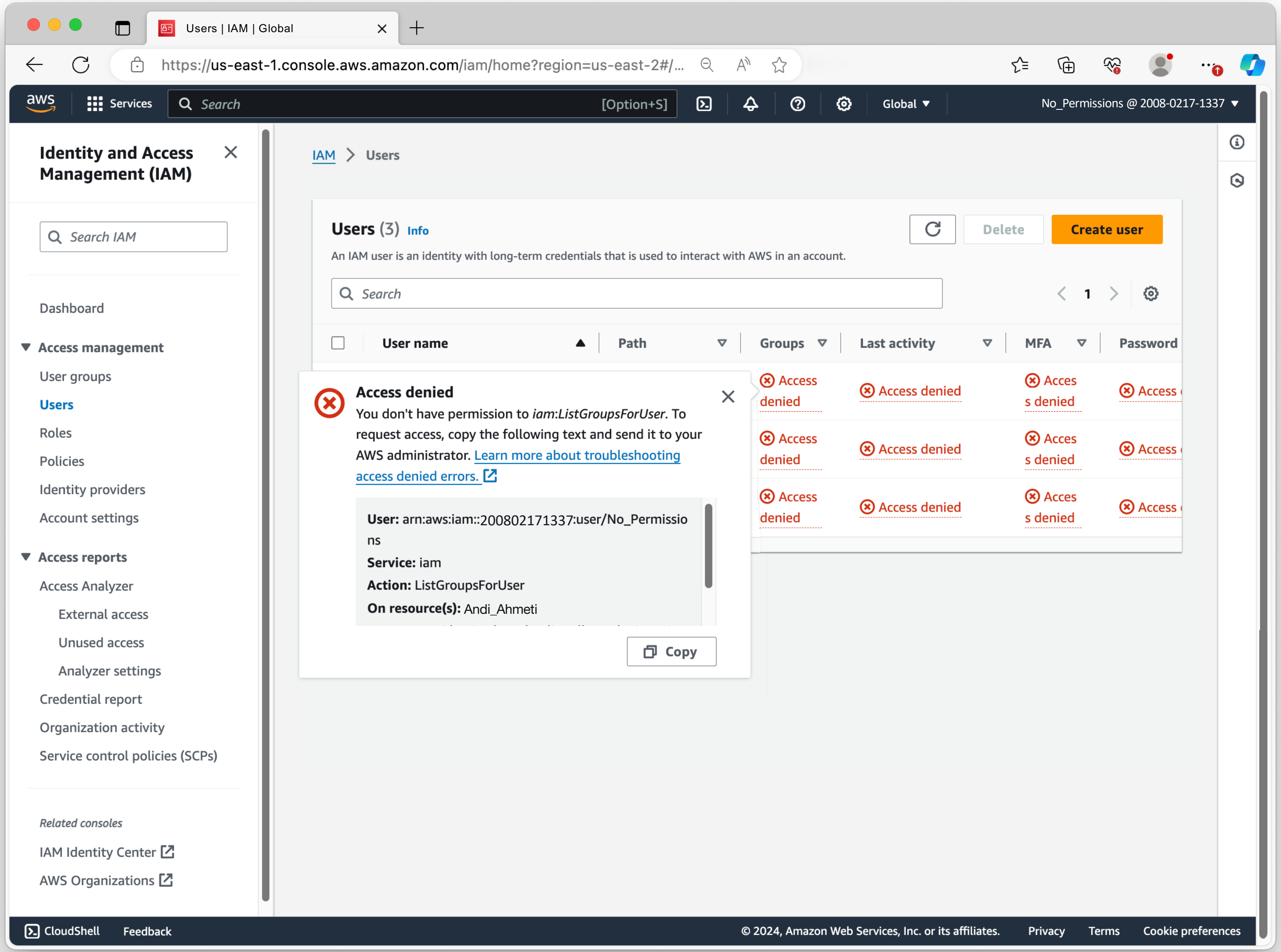


No Permissions – 3/3 – IAM Users



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

No Permissions – 3/3 – IAM Users



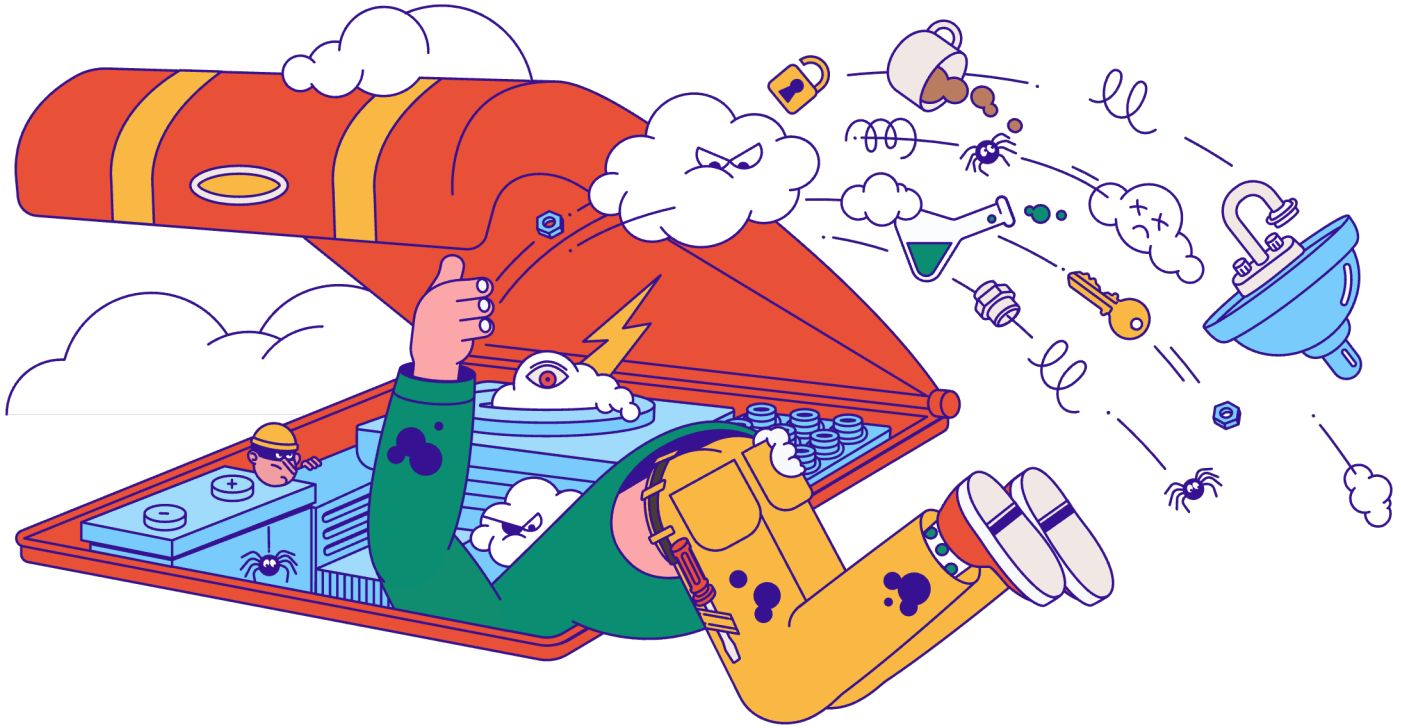
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "iam:ListUsers",
      "Resource": "*"
    }
  ]
}
```

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.

Delete | Create user

Search

1

User name	Path	Groups	Last activity	MFA	Password

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.

Copy

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

B

Users (3) Info

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

Delete | Create user

Search

1

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

C

Users (3) Info

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

Delete | Create user

Search

1

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

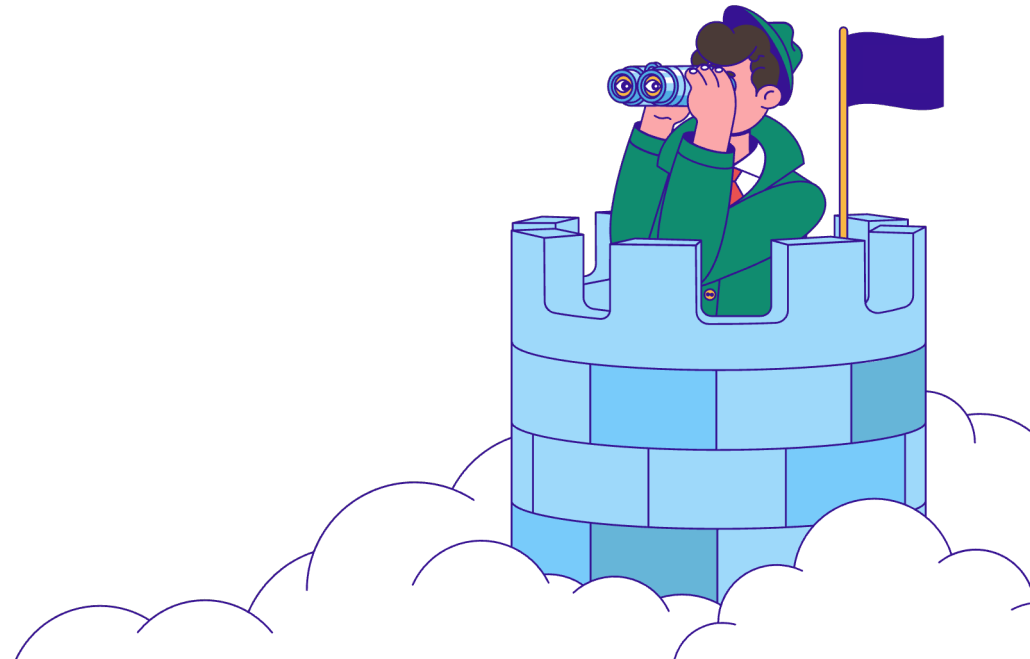
Console Mapping – IAM Users

A

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

B

C



Console Mapping – IAM Users

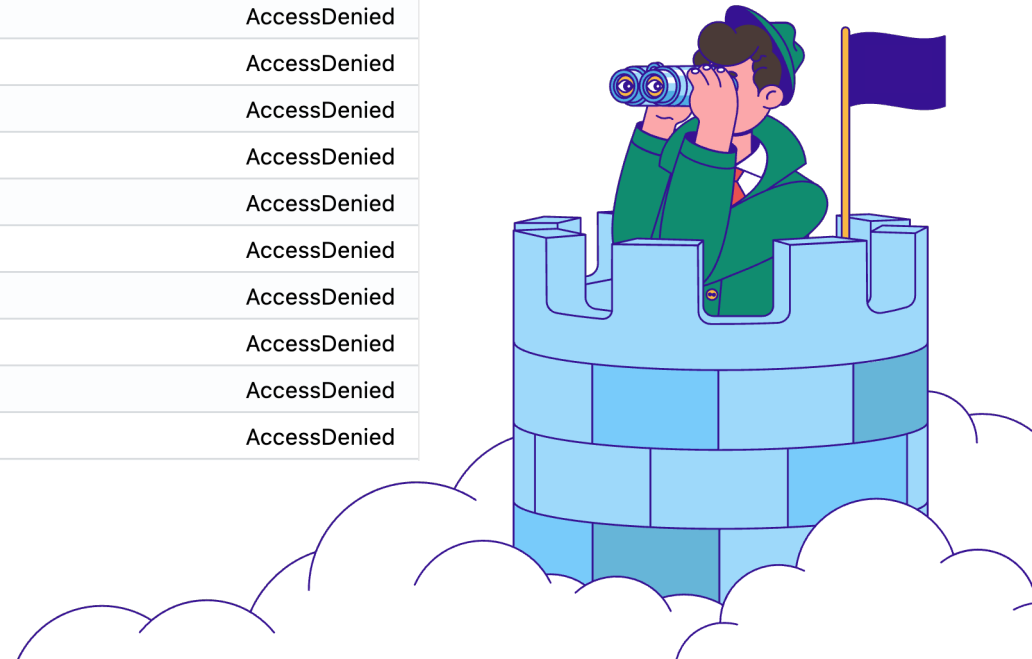
A

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

B

C

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



Console Mapping – IAM Users

A

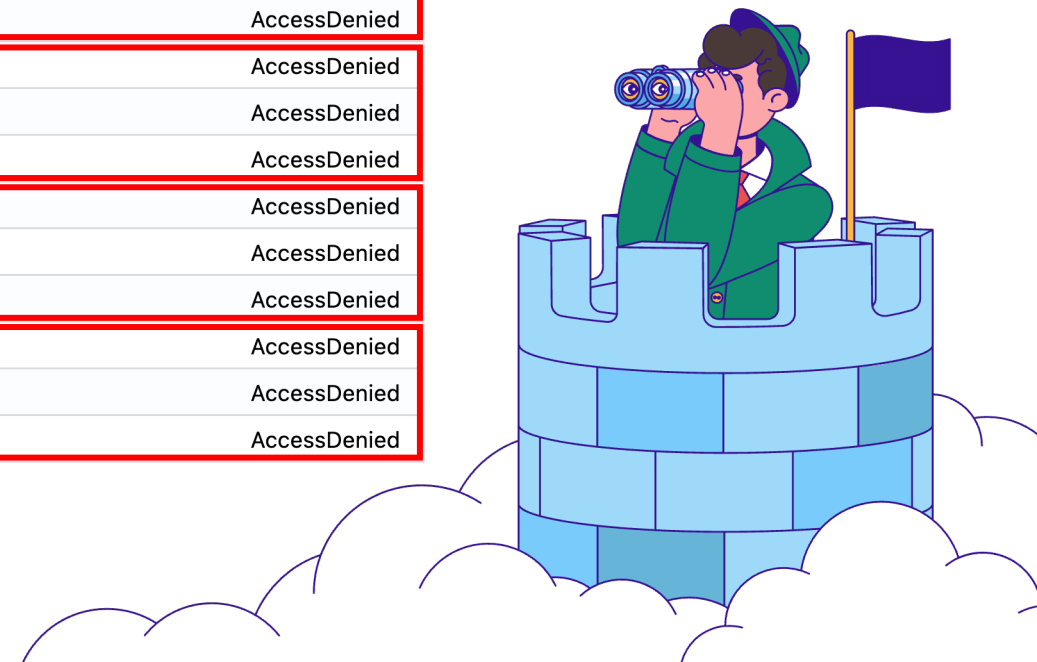
eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:13:37.0000	iam:ListUsers	AWS Internal		AccessDenied

B

eventTime	eventNameFull	userAgent	requestParameters	errorCode
2024-03-18 04:17:16.0000	iam:ListUsers	AWS Internal	{"maxItems":1000}	

C

eventTime	eventNameFull	userAgent	requestParameters	errorCode
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

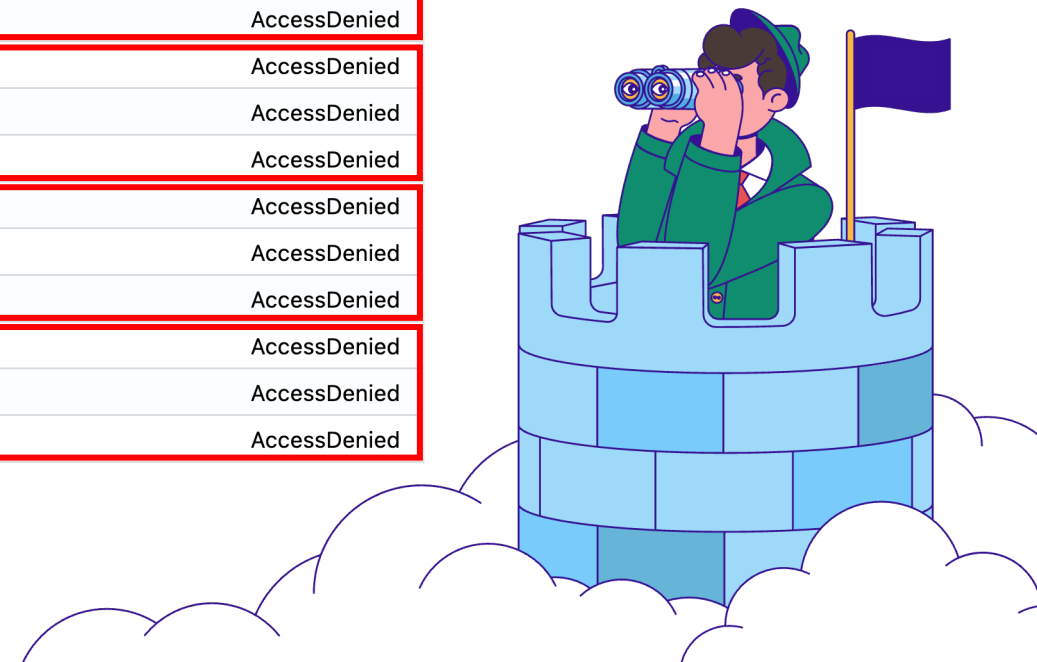
A

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

B

C

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



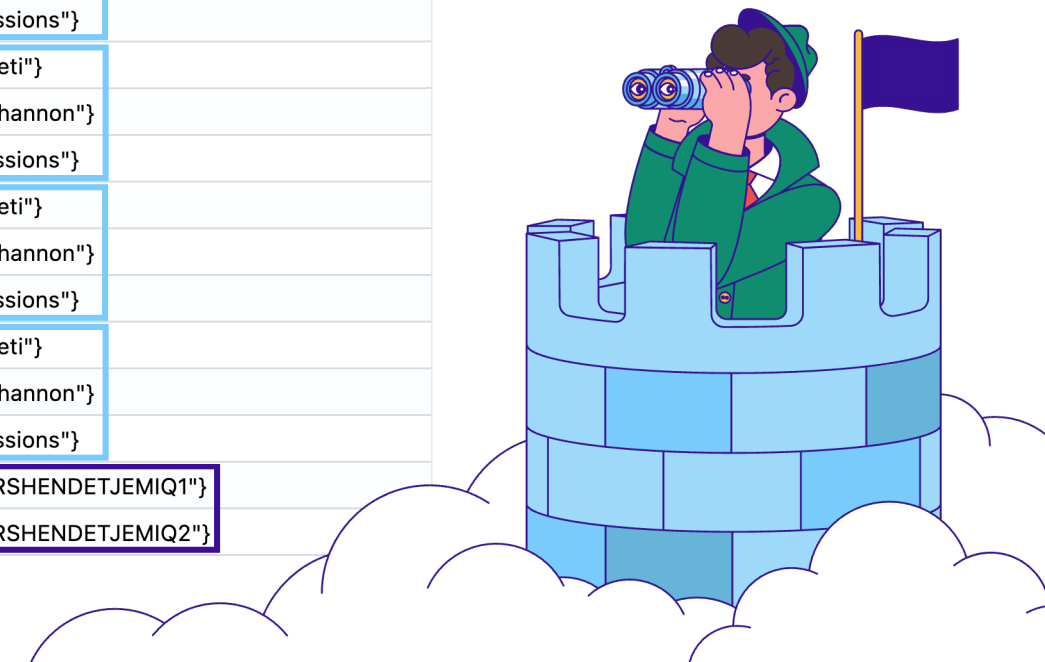
Console Mapping – IAM Users

A

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

C

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

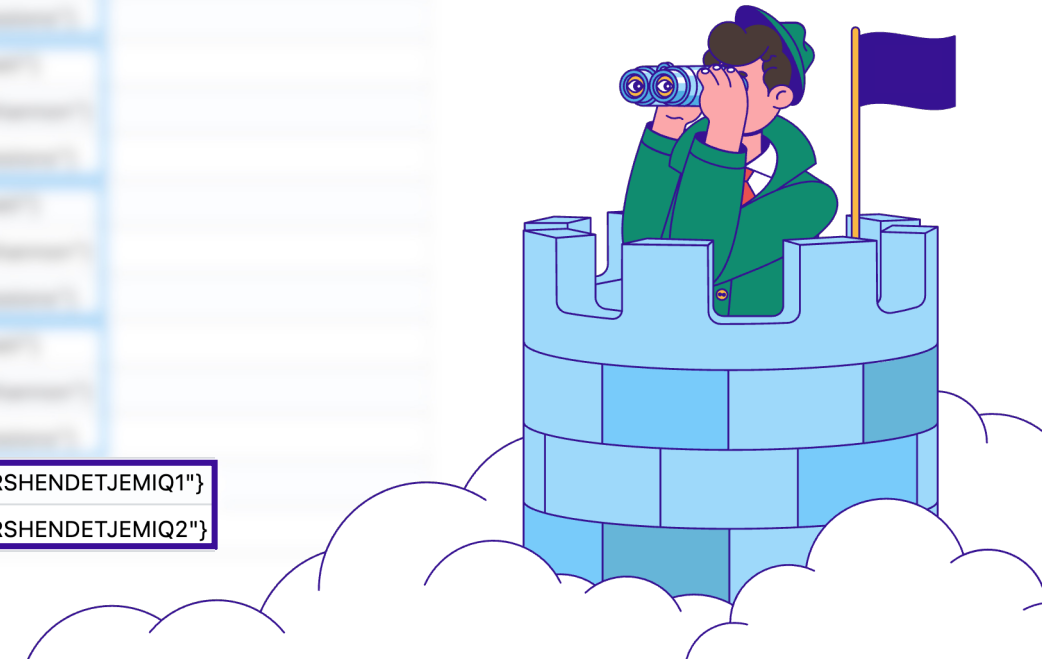


Console Mapping – IAM Users

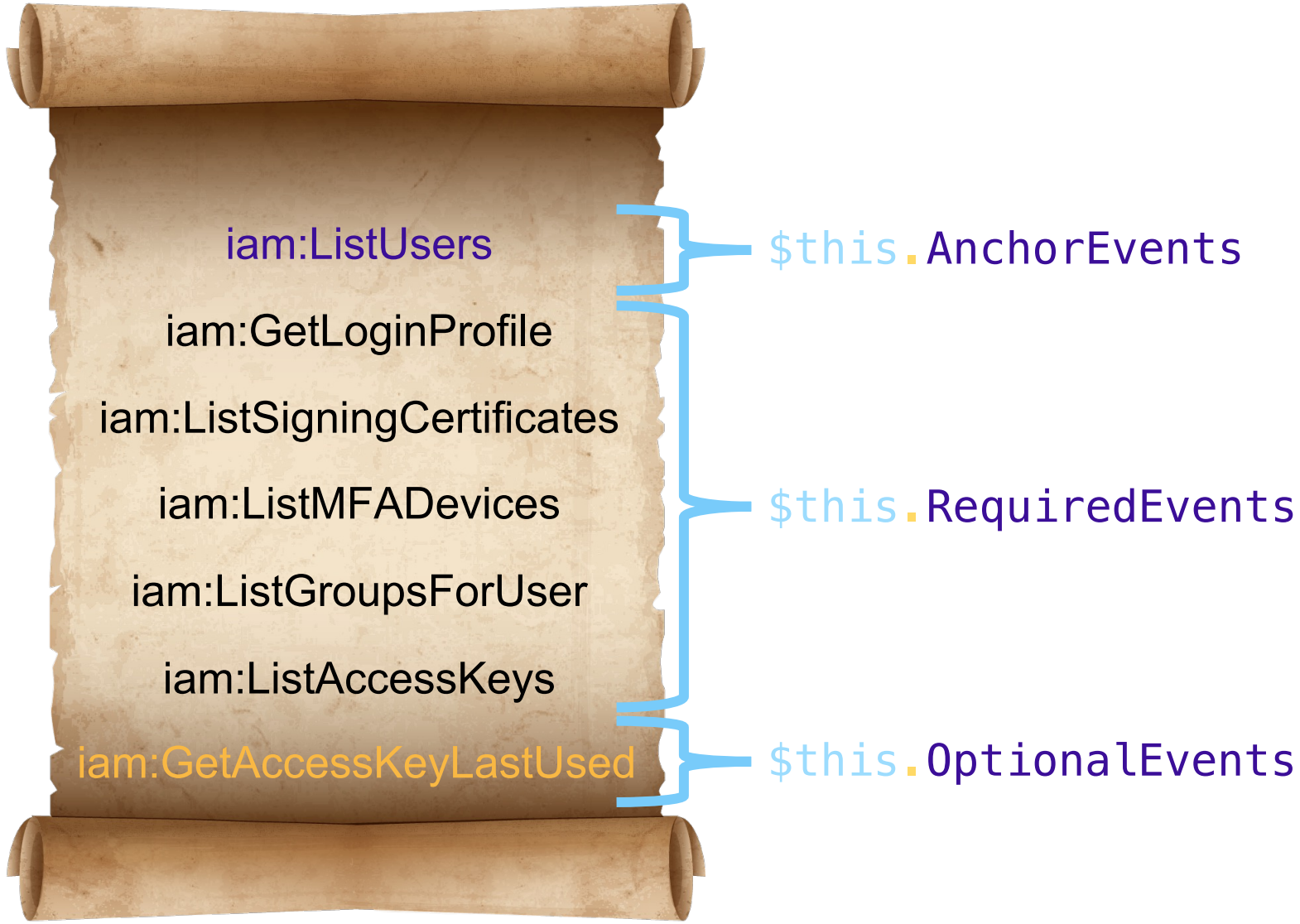
A

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

Console Mapping – OptionalEvents (Background)

ConsoleHome

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

Console Mapping – OptionalEvents (Background)

ConsoleHome

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

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

Console Mapping – OptionalEvents (Background)

ConsoleHome

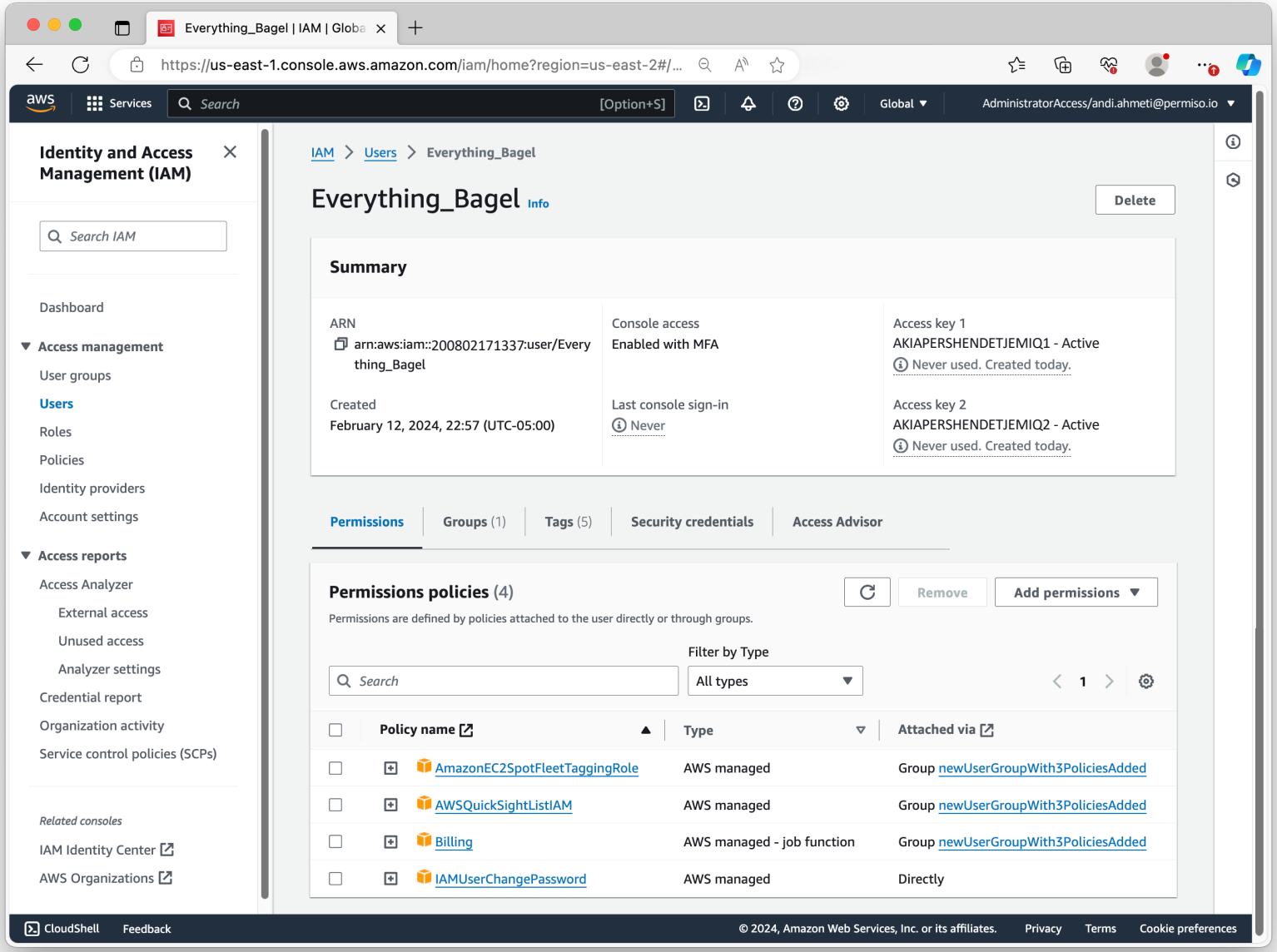
eventTime	eventNameFull	userAgent	requestParameters
2024-03-18 04:19:43.0000	ec2:DescribeRegions	Mozilla/5.0 (Macintosh; Intel ...	{"regionSet":{},"allRegions":true}
2024-03-18 04:19:44.0000	ce:GetCostAndUsage	Mozilla/5.0 (Macintosh; Intel ...	{"Filter":{"Not":{"Or":[{"Dimensions":{"V
2024-03-18 04:19:44.0000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

Console Mapping – OptionalEvents (Context)

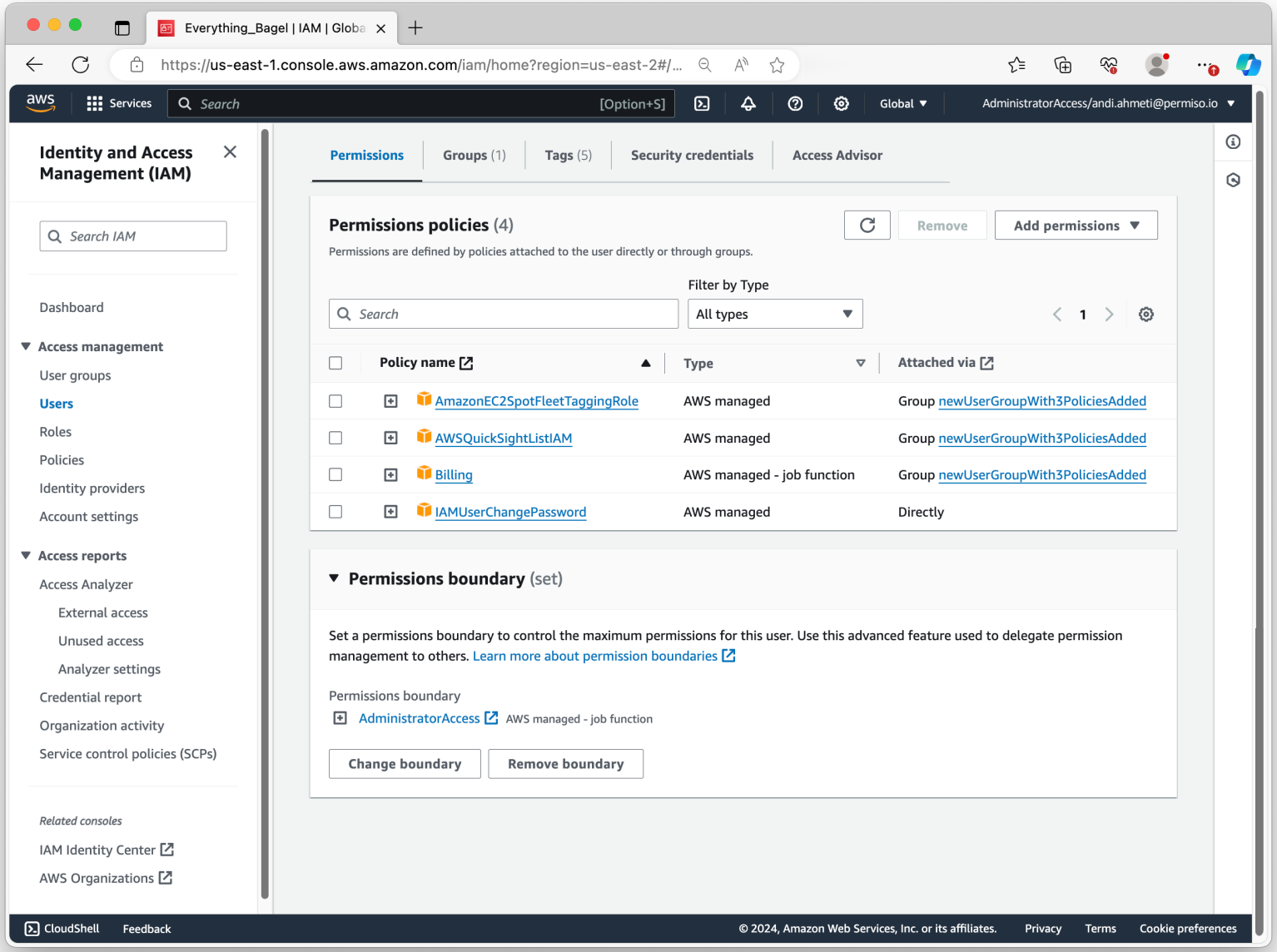
EVERYTHING_BAGEL

PLAIN_BAGEL

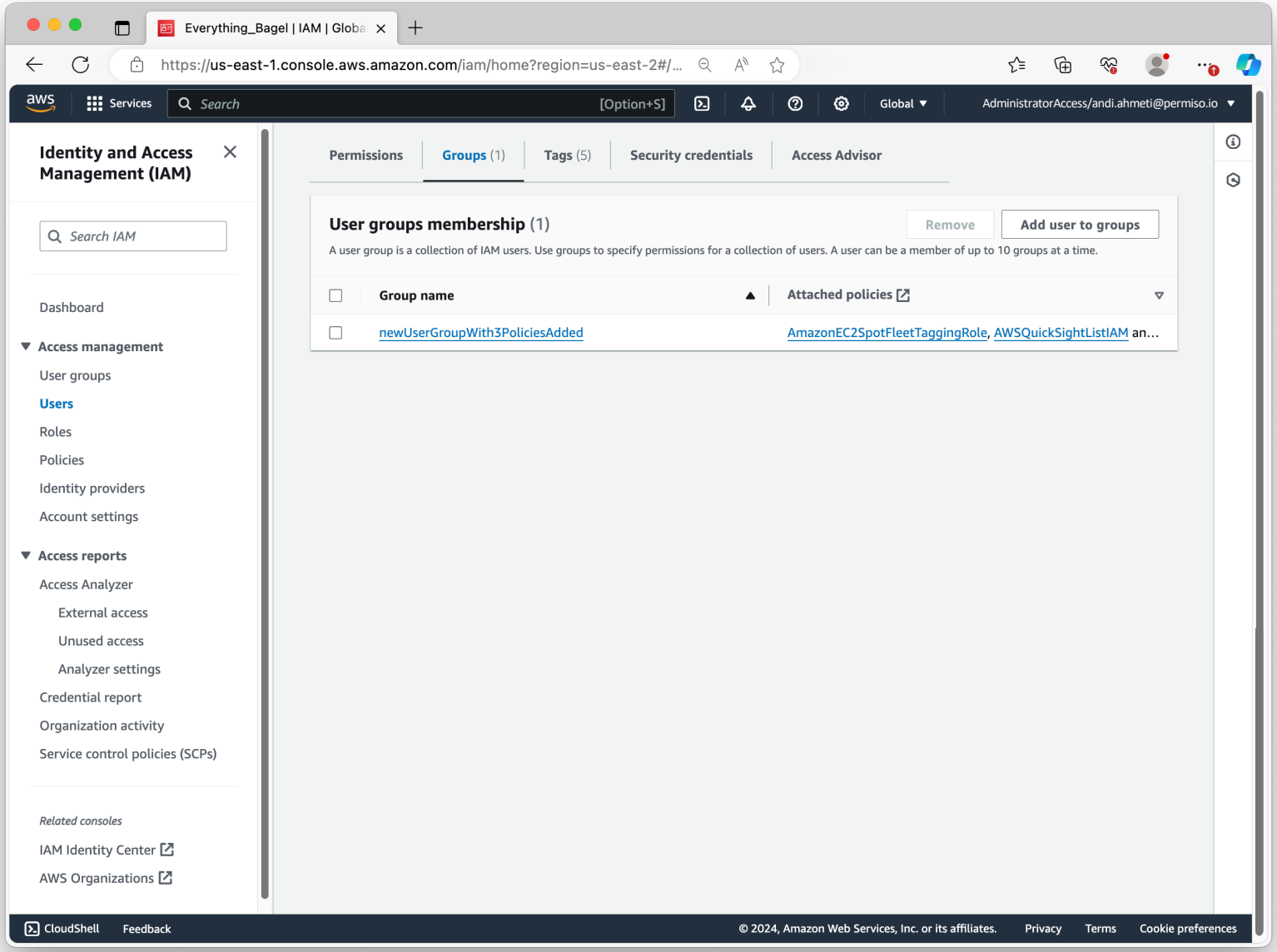
Console Mapping – OptionalEvents (Context)



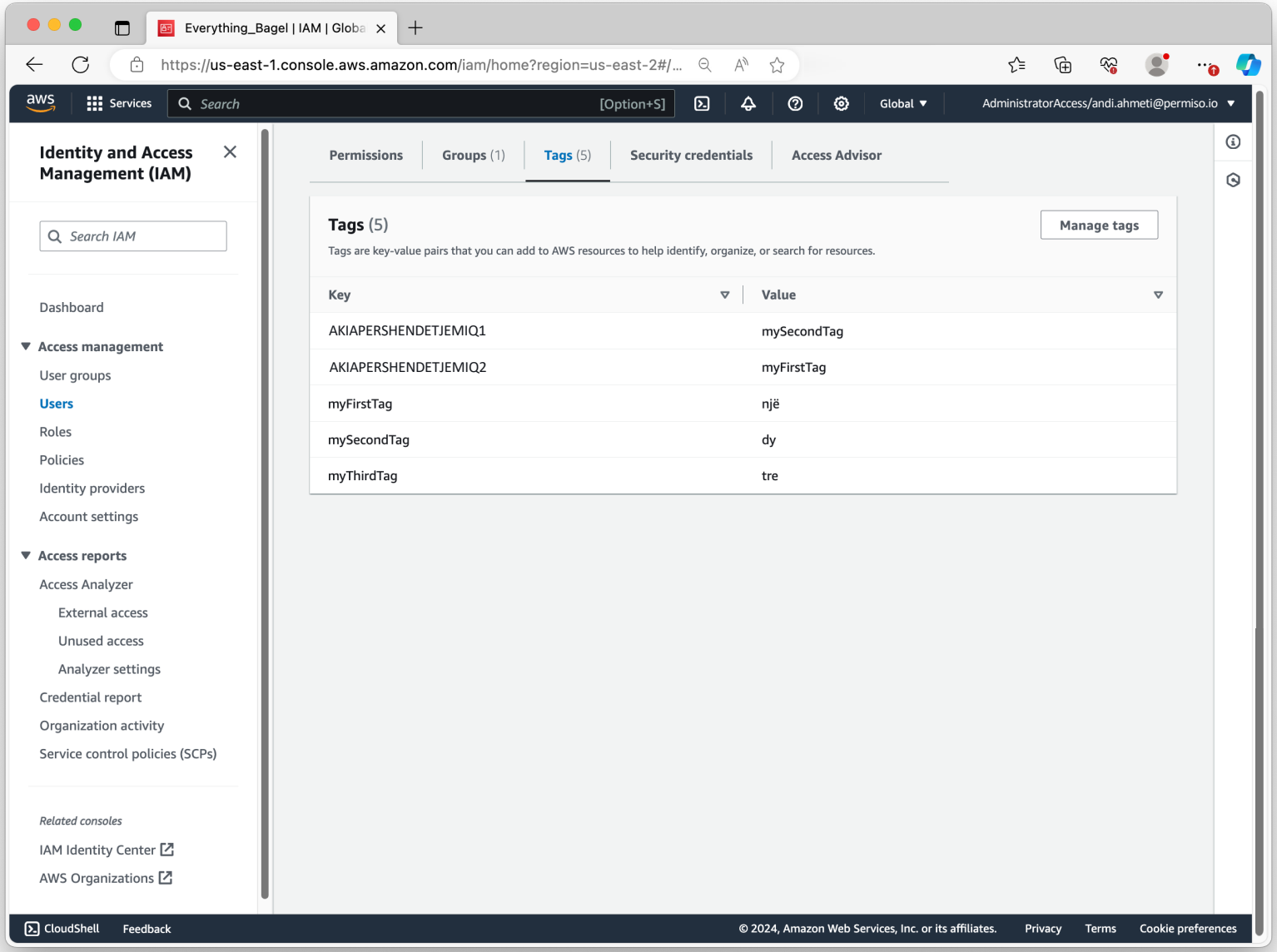
Console Mapping – OptionalEvents (Context)



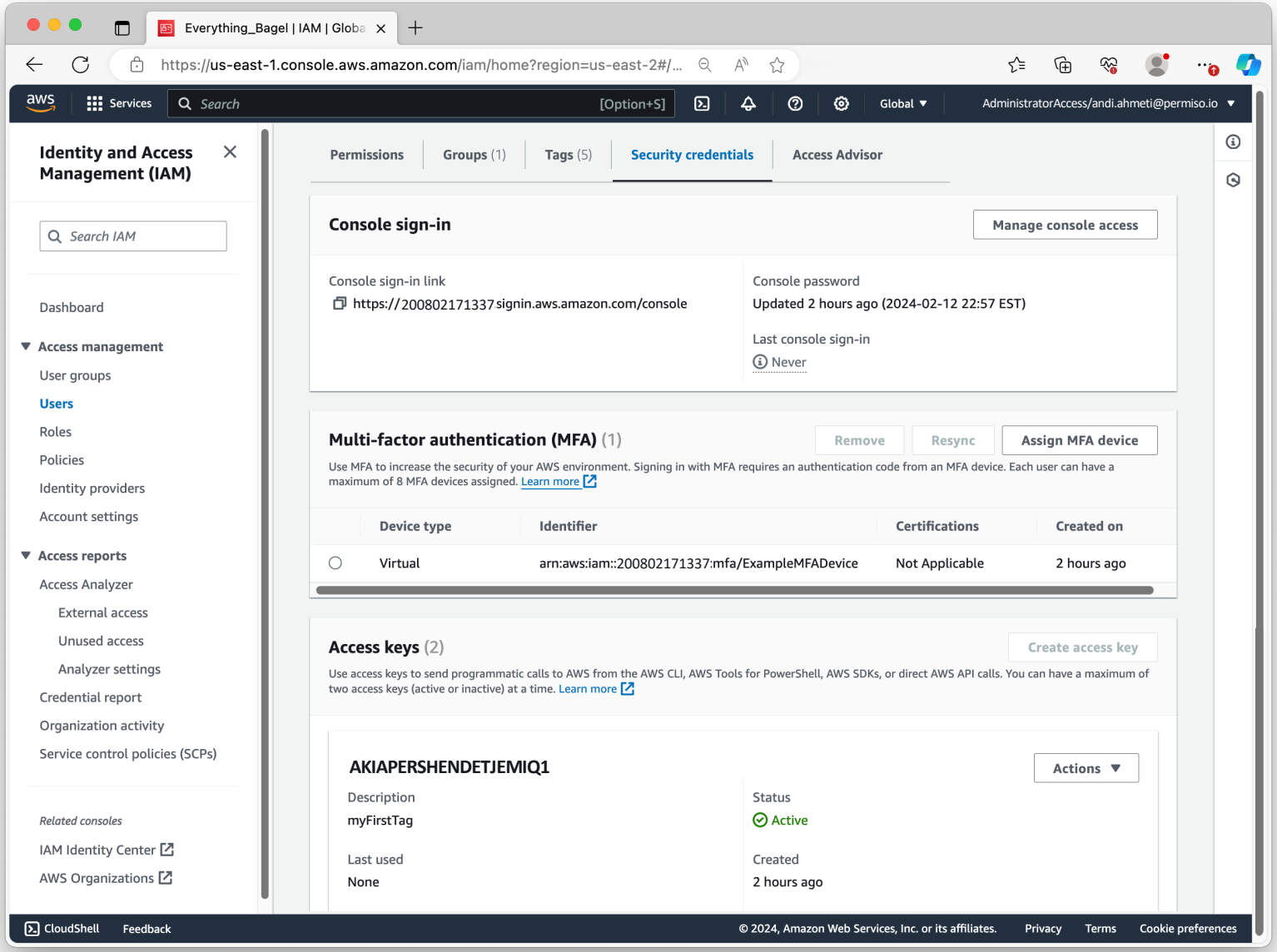
Console Mapping – OptionalEvents (Context)



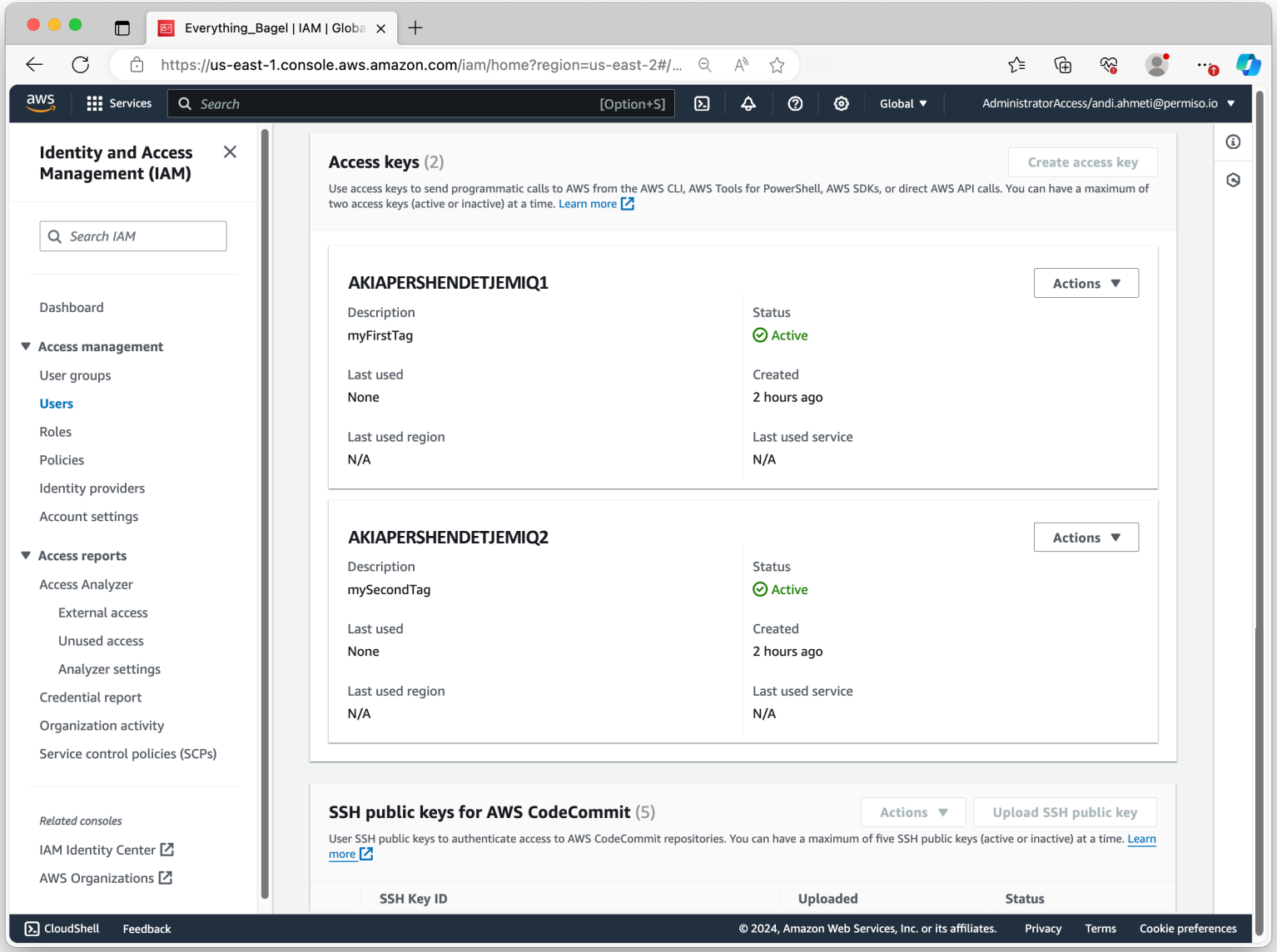
Console Mapping – OptionalEvents (Context)



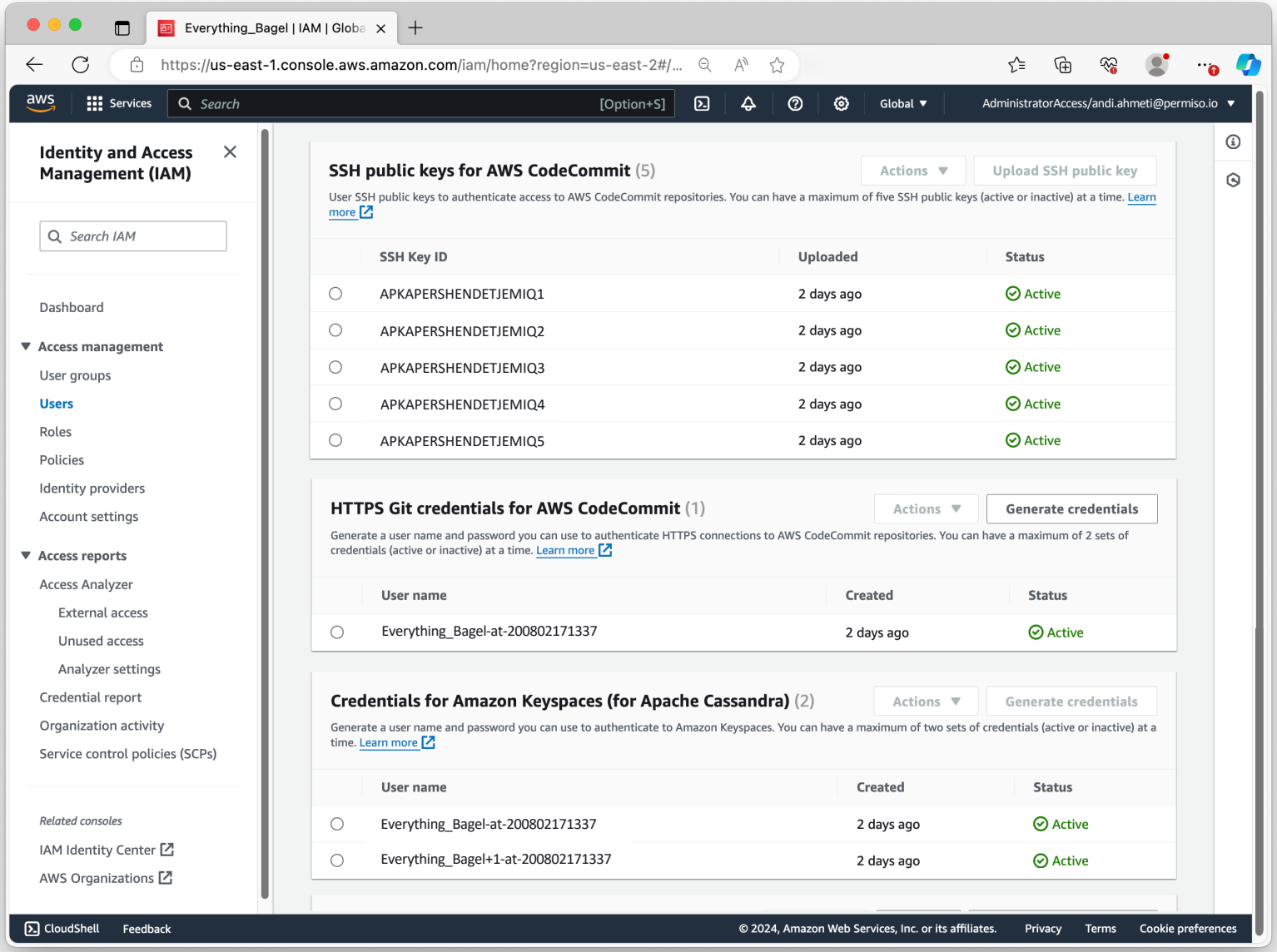
Console Mapping – OptionalEvents (Context)



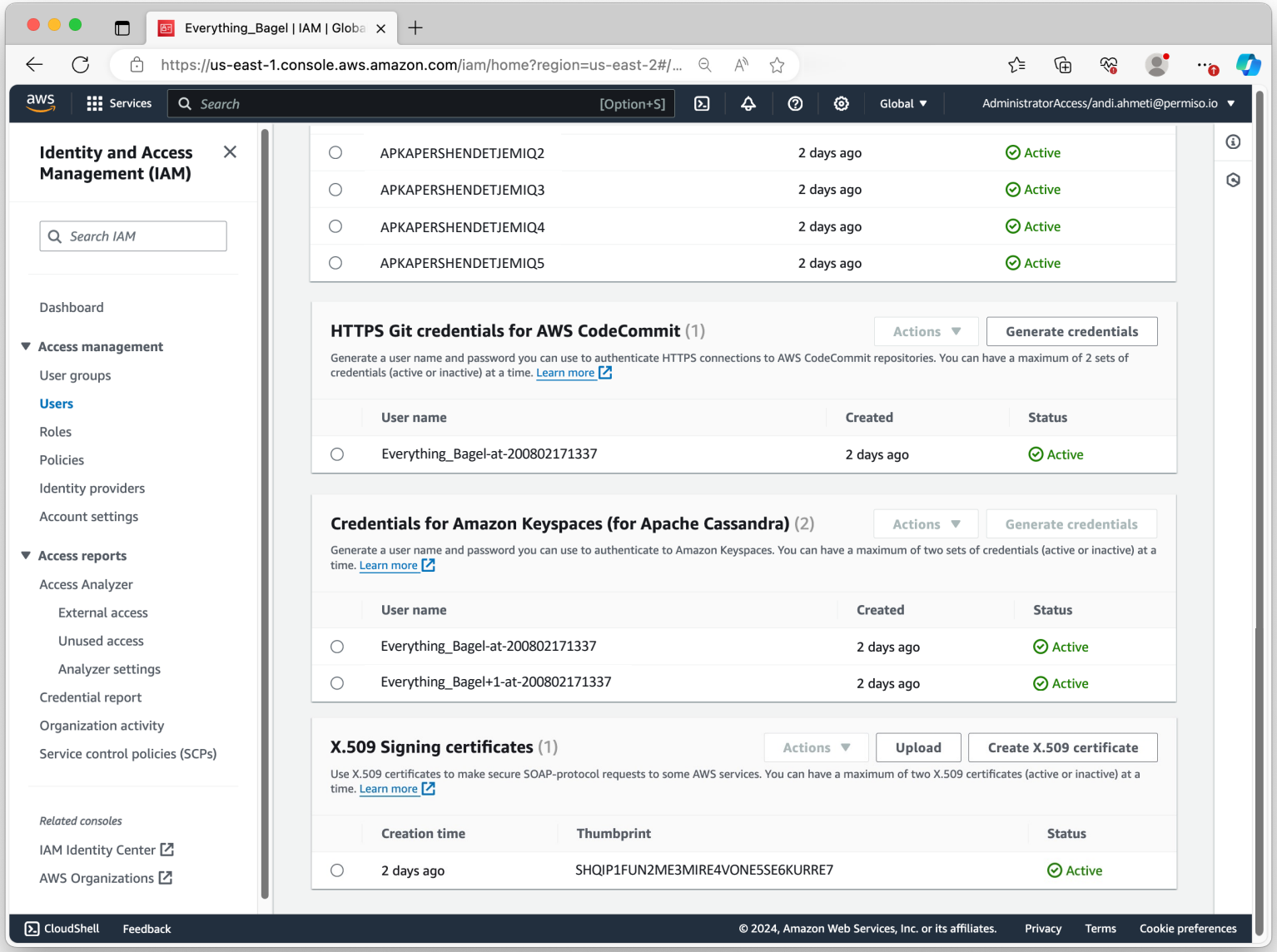
Console Mapping – OptionalEvents (Context)



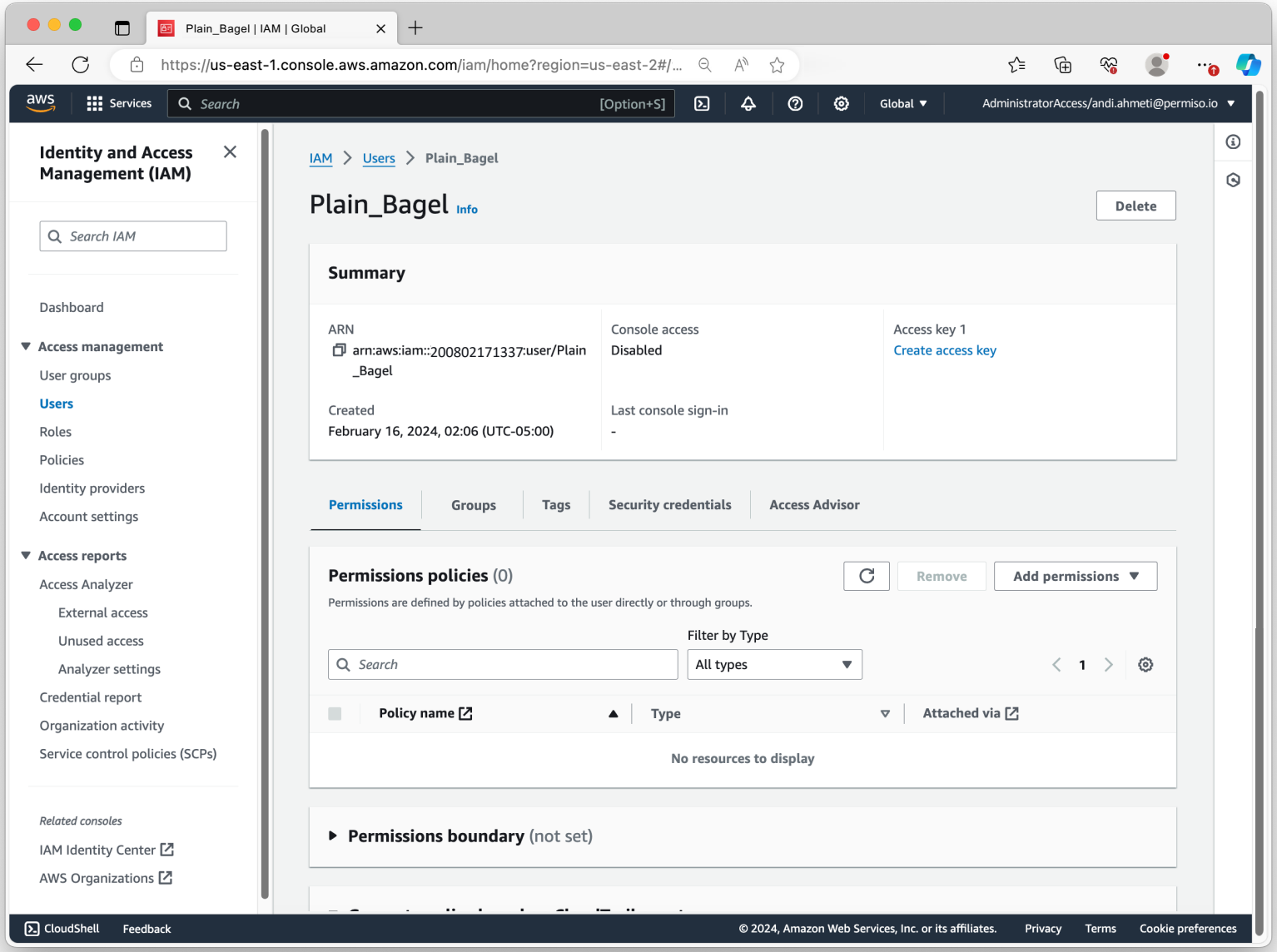
Console Mapping – OptionalEvents (Context)



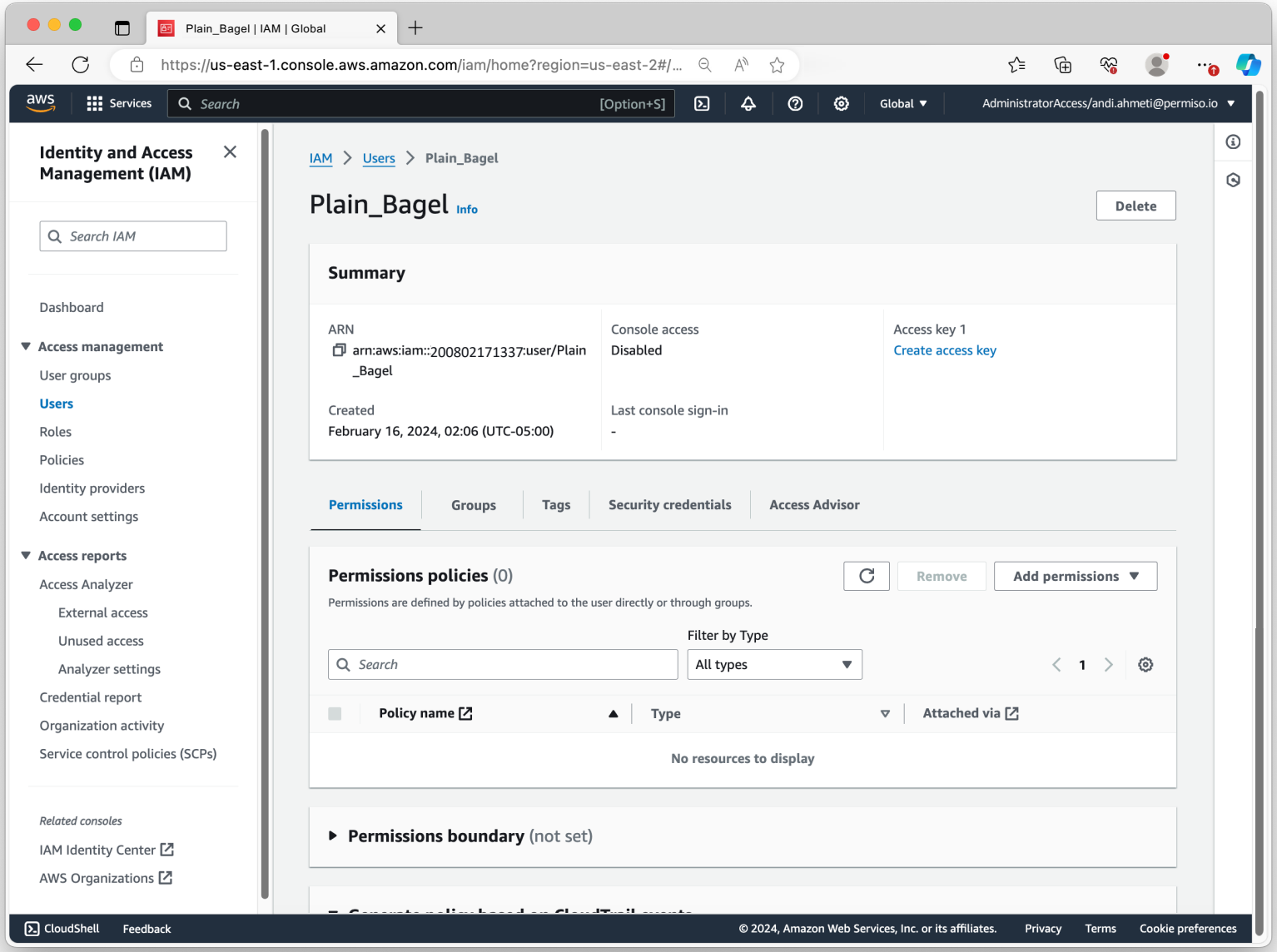
Console Mapping – OptionalEvents (Context)



Console Mapping – OptionalEvents (Context)



Console Mapping – OptionalEvents (Context)



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":"AAl1zjUVlnJUxBcsOtgybPoPxBF...
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)

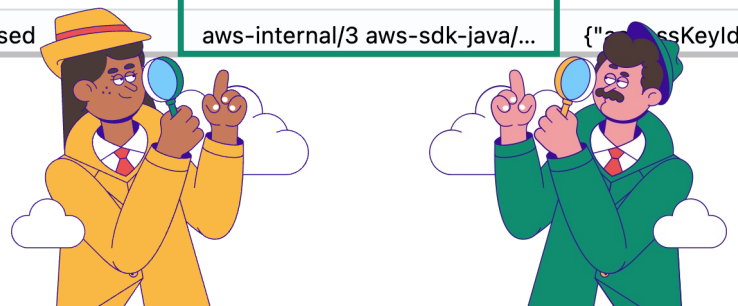
Permissions | Groups | Tags | Security credentials | Access Advisor

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	iam:ListGroupPolicies	AWS Internal	{"groupName":"customGroup2"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:ListAttachedGroupPolicies	AWS Internal	{"groupName":"customGroup2"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:GetLoginProfile	aws-internal/3 aws-sdk-java/...	{"userName":"Everything_Bagel"}
2024-03-18 04:21:20.0000	2024-03-18 04:24:43.0000	access-analyzer:ListPolicyGenerations	aws-internal/3 aws-sdk-java/...	{"principalArn":"arn:aws:iam::200802171337:user/Everything_Bagel"}
2024-03-18 04:21:21.0000	2024-03-18 04:24:43.0000	iam:ListAccessKeys	AWS Internal	{"userName":"Everything_Bagel"}
	2024-03-18 04:24:44.0000	iam:ListAccessKeys	aws-internal/3 aws-sdk-java/...	{"userName":"Everything_Bagel"}
	2024-03-18 04:24:44.0000	iam:GetAccessKeyLastUsed	AWS Internal	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:44.0000	iam:GetAccessKeyLastUsed	AWS Internal	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}
	2024-03-18 04:24:45.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ1"}
	2024-03-18 04:24:45.0000	iam:GetAccessKeyLastUsed	aws-internal/3 aws-sdk-java/...	{"accessKeyId":"AKIAPERSHENDETJEMIQ2"}

Console Mapping – OptionalEvents (Context)

Permissions | Groups | Tags | Security credentials | Access Advisor

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



Console Mapping – OptionalEvents (Context)

Permissions | Groups | Tags | Security credentials | Access Advisor

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

Console Mapping – 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
iam:ListGroupPolicies
iam:ListAttachedGroupPolicies
iam:GetAccessKeyLastUsed

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

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

Console Mapping – OptionalEvents (Context)

iam:ListPolicies

Permissions | Groups | Tags | Security credentials | Access Advisor

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

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

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

Console Mapping – 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:GetAccessKeyLastUsed
iam:GetAccessKeyLastUsed

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

Console Mapping – OptionalEvents (Context)

iam:ListPolicies

Permissions | Groups | Tags | Security credentials | Access Advisor

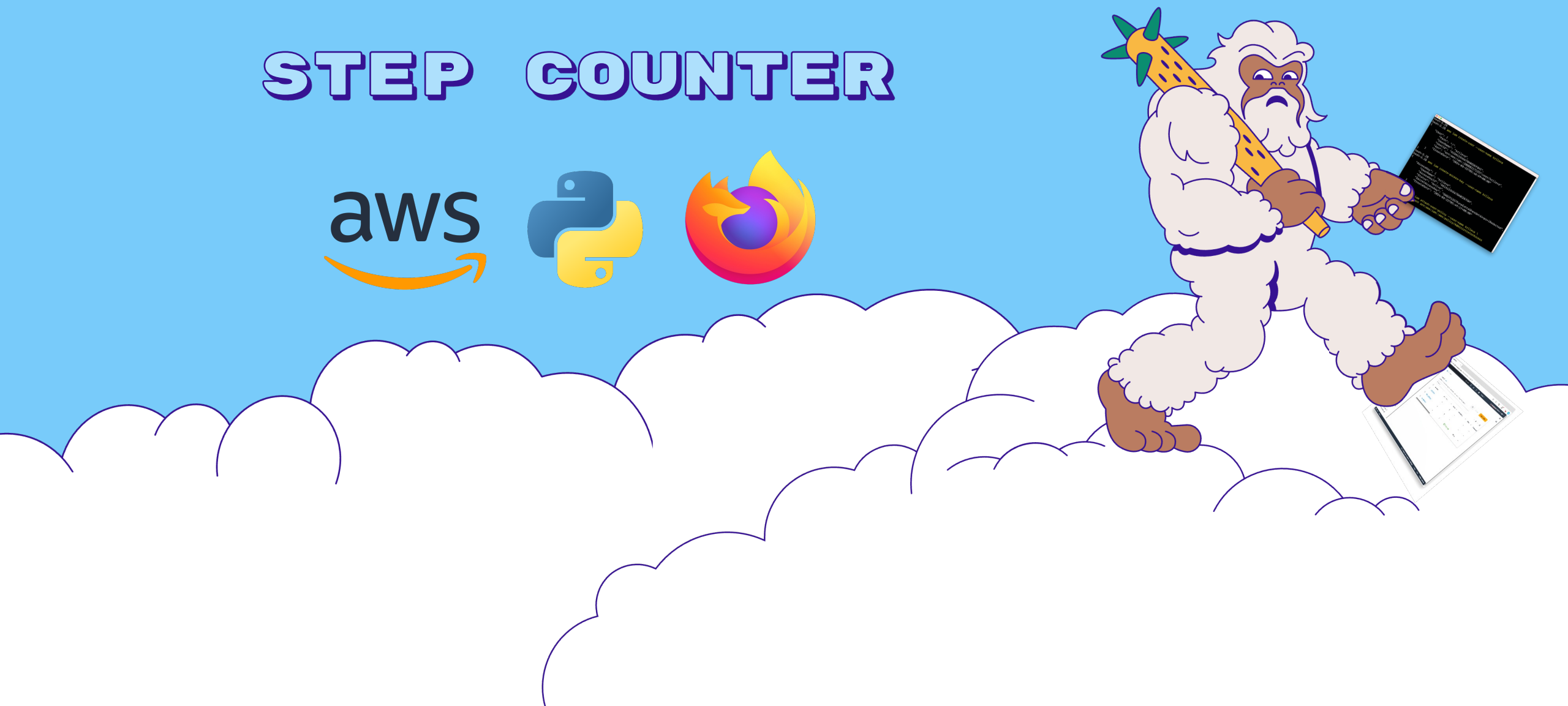
eventNameFull
iam:ListAccessKeys
iam:ListSigningCertificates
iam:ListSSHPublicKeys
iam:ListServiceSpecificCredentials
iam:ListServiceSpecificCredentials

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

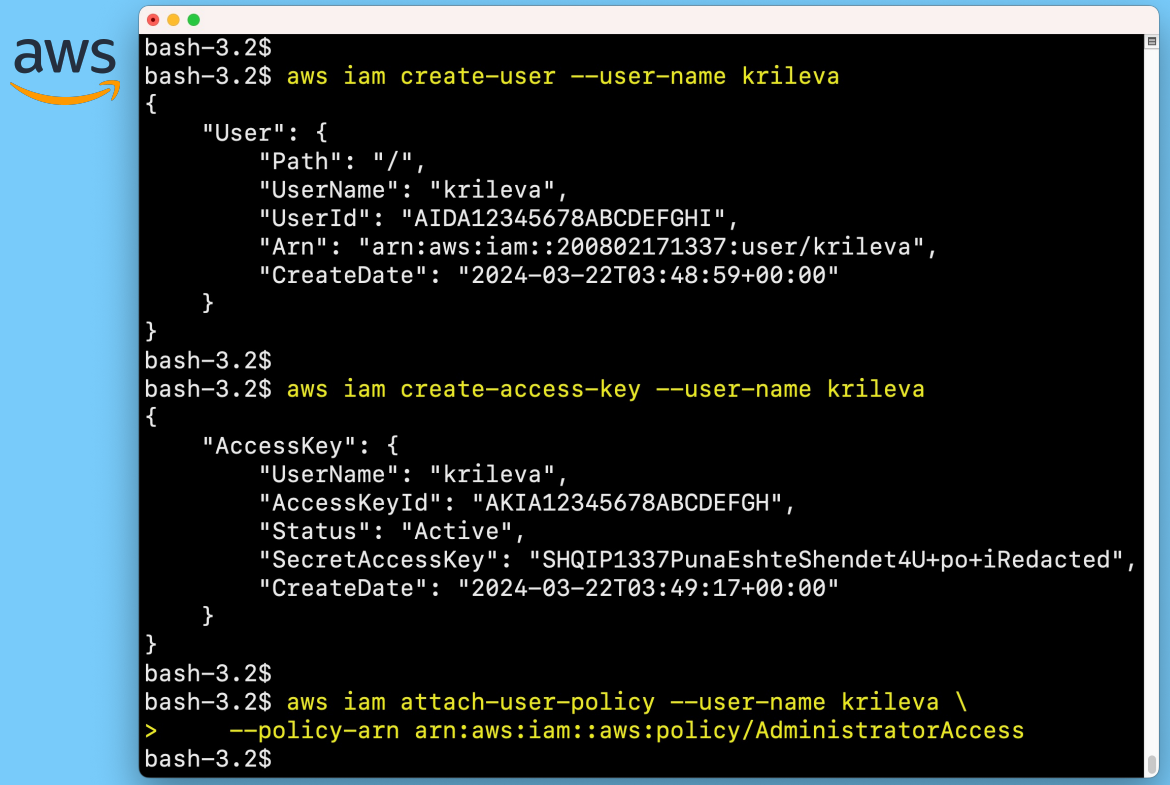
- iam:GetPolicy
- iam:ListGroupPolicies
- iam:ListAttachedGroupPolicies
- iam:GetAccessKeyLastUsed

CLI vs Console

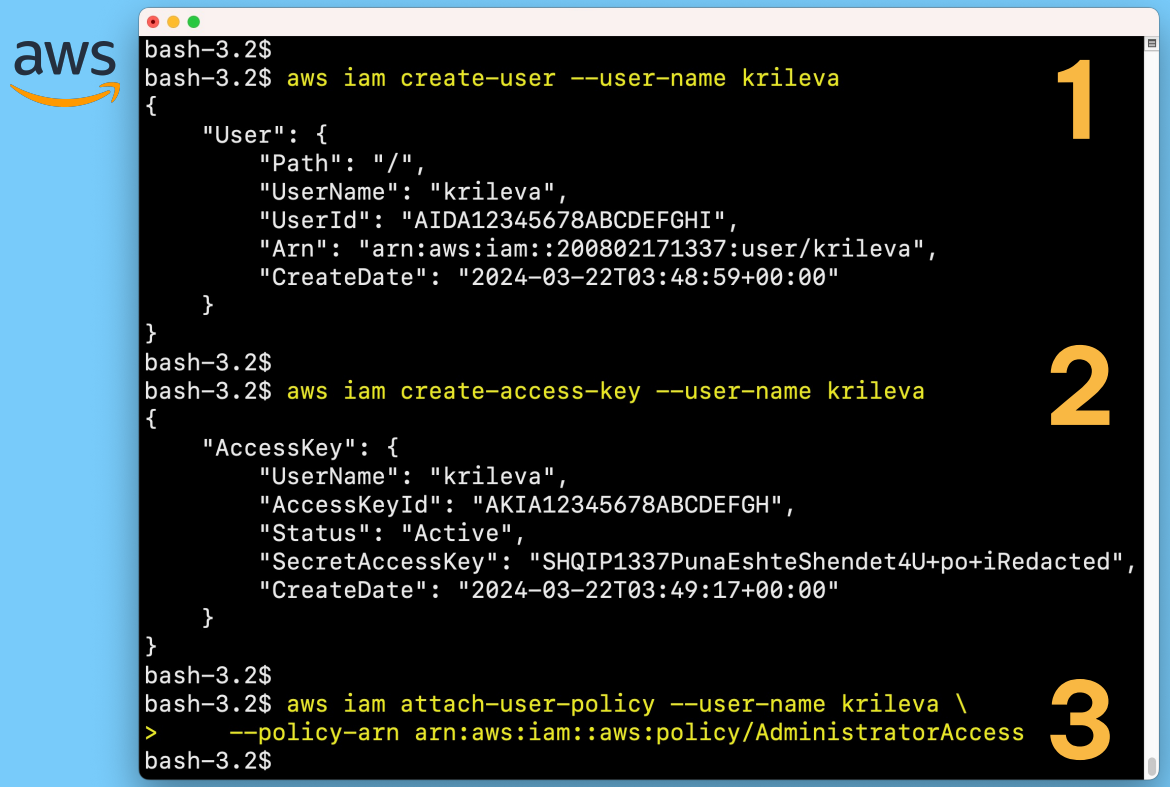
STEP COUNTER



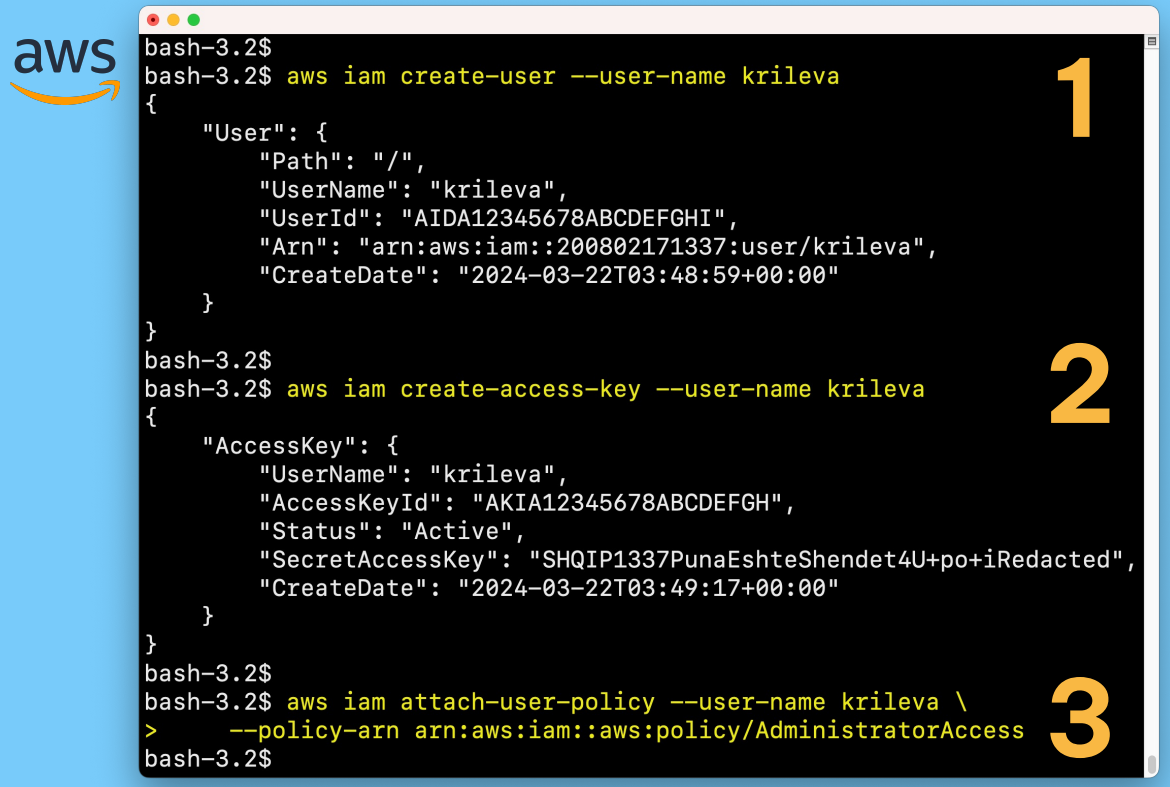
CLI vs Console



CLI vs Console



CLI vs Console



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': 'AIDA12345678ABCDEFGHI',
 'UserName': 'krileva'}

iam_client.create_access_key(UserName=krileva)

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

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

bash-3.2$
```

1

2

3

```python
import boto3
from pprint import pprint

# Define IAM client
iam_client = boto3.client('iam')

# Specify username for new IAM User
username = 'krileva'

# Specify policy ARN to add to newly created IAM User
policyArn = "arn:aws:iam::aws:policy/AdministratorAccess"

# Create IAM User
response = iam_client.create_user(UserName=username)
print(f"\niam_client.create_user(UserName={username})\n")
pprint (response['User'])

# Create Access Key for newly created IAM User
response = iam_client.create_access_key(UserName=username)
print(f"\niam_client.create_access_key(UserName={username})\n")
pprint (response['AccessKey'])

# Attach policy to newly created IAM User
response = iam_client.attach_user_policy(UserName=username,PolicyArn=policyArn)
print(f"\niam_client.attach_user_policy(UserName={username},PolicyArn={policyArn})\n")

```

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': 'AIDA12345678ABCDEFGHI',
 'UserName': 'krileva'}

iam_client.create_access_key(UserName=krileva)

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

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

bash-3.2$
```

1

2

3

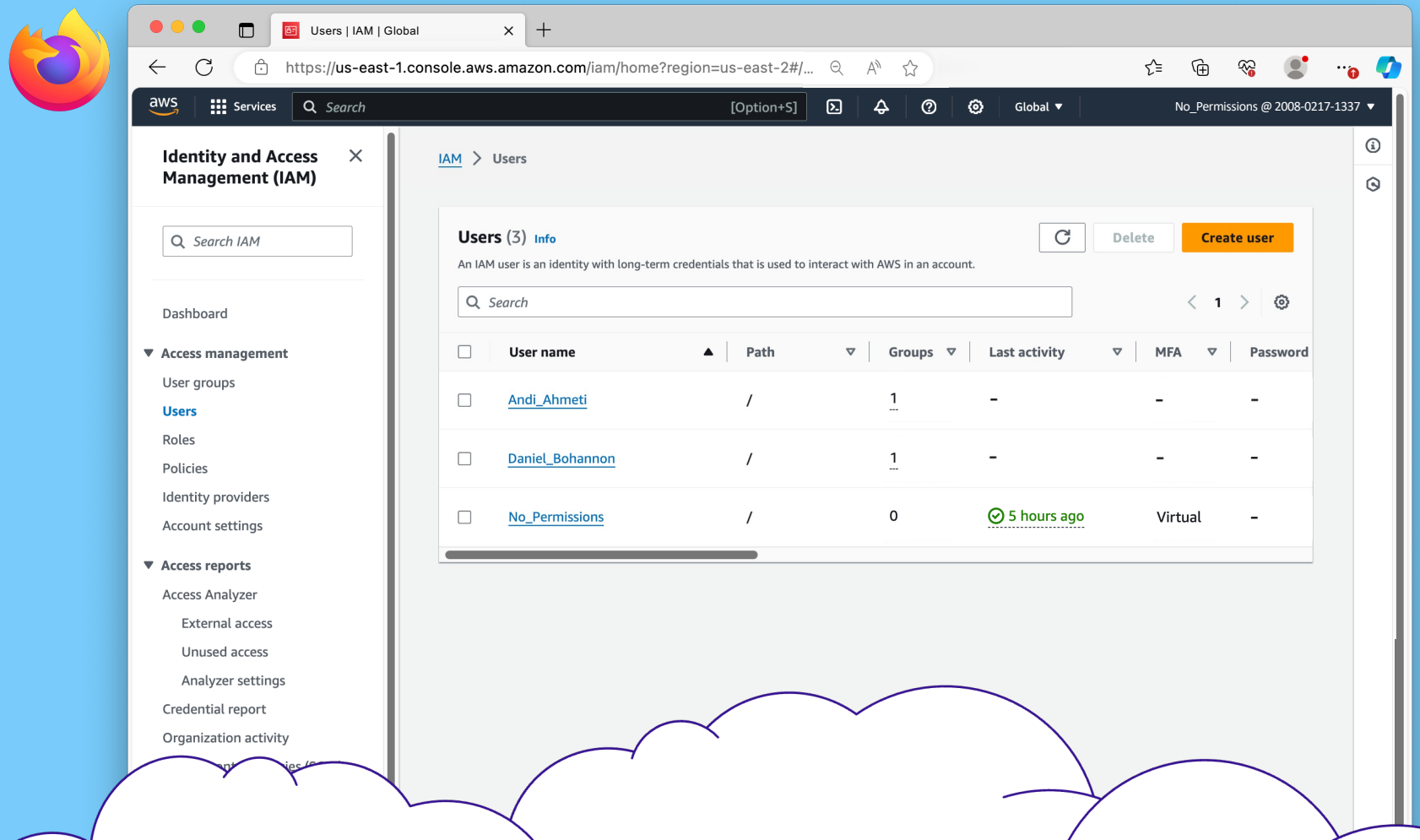
eventNameFull	requestParameters
iam:CreateUser	{"userName":"krileva"}
iam:CreateAccessKey	{"userName":"krileva"}
iam:AttachUserPolicy	{"userName":"krileva","policyArn":"arn:aws:iam::aws:policy/AdministratorAccess"}

```python
import boto3
from pprint import pprint

# Define IAM client
iam_client = boto3.client('iam')

# Specify username for new IAM User
username = 'krileva'

# Specify policy ARN to add to newly created IAM User
policyArn = "arn:aws:iam::aws:policy/AdministratorAccess"

# Create IAM User
response = iam_client.create_user(UserName=username)
print(f"\niam_client.create_user(UserName={username})\n")
pprint (response['User'])

# Create Access Key for newly created IAM User
response = iam_client.create_access_key(UserName=username)
print(f"\niam_client.create_access_key(UserName={username})\n")
pprint (response['AccessKey'])

#                                    ewly created IAM User
                                    attach_user_policy(UserName=username,Pol
                                    licy(UserName={username},Po
```

1

2

CLI vs Console



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		rameters
			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-int... aws-sdk-java/...	{"userName":"Daniel_Bohannon"}
2024-03-22 04:55:34.0000	iam:ListAccessKeys	...-java/...	{"userName":"No_Permissions"}
...000	iam:GetAcce...	...va/...	...KeyId":"AKIAPERSHENDETJEMIQ1"}
	...GetA...		...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	

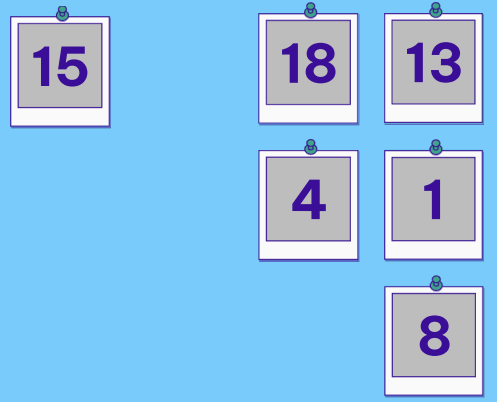
IAM_Users_CreateUser_Step1B (attach policy)

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	aw -sdk-java/...	{"groupName":"customGroup2"}
2024-03-22 04:56:25.0000	iam:ListPolicies	java/...	{"scope":"AWS","onlyAttached":false,"pathPrefix":"/"}
	iam:ListPoli	va/...	S","onlyAttached":false,"pathPrefix":"/"}
			ws:iam::200802171337:policy/Per...
			71337:policy/Per...
			37:policy/p

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...



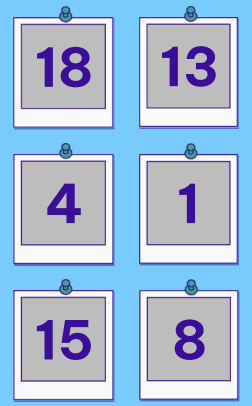
CLI vs Console

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:...

IAM_Users_SPECIFICUSER_Permissions

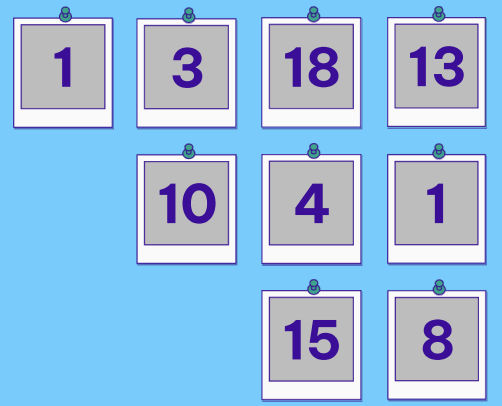
eventTime	eventNameFull	userAgent	requestParameters
2024-03-22 04:57:59.0000	iam:ListUserTags	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:ListUserPolicies	AWS Internal	{"userName":"krileva"}
2024-03-22 04:57:59.0000	iam:ListMFADevices	AWS Internal	{"userName":"krileva"}
2024-03-22 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	aw...	-sdk-java/... {"userName":"krileva"}
2024-03-22 04:58:00.0000	iam:ListAccessKeys		iava/... {"userName":"krileva"}
	access-ana		a/... ":"arn:aws:iam::200802171337:user/kri...



CLI vs Console

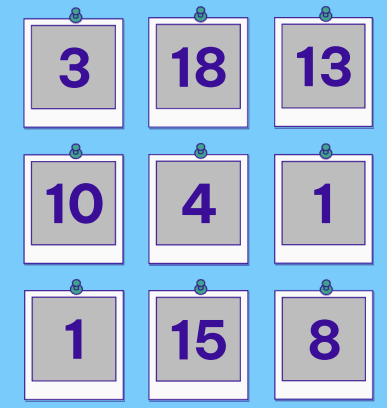
IAM_Users_SPECIFICUSER_CreateAccessKey

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



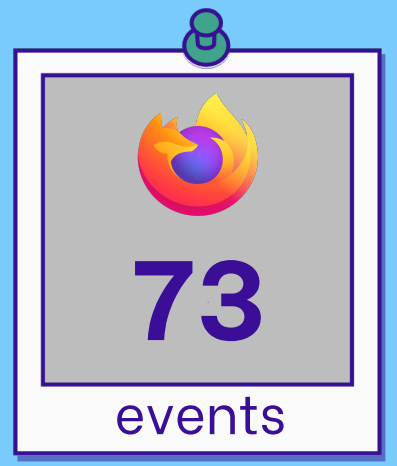
CLI vs Console

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



CLI vs Console

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



CLI vs Console

Worst Case Scenarios

$n=3$

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

IAM_Users

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

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

IAM_Users

n=20

Page size
- (•) 20 rows
- ( ) 50 rows
- ( ) 100 rows

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

$1+5(20)+[0,2(20)]=$ **141**

n=50

Page size
- ( ) 20 rows
- (•) 50 rows
- ( ) 100 rows

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

$1+5(50)+[0,2(50)]=$ **351**

n=100

Page size
- ( ) 20 rows
- ( ) 50 rows
- (•) 100 rows

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

$1+5(100)+[0,2(100)]=$ **701**

Worst Case Scenarios

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

$21+4n$

n=100

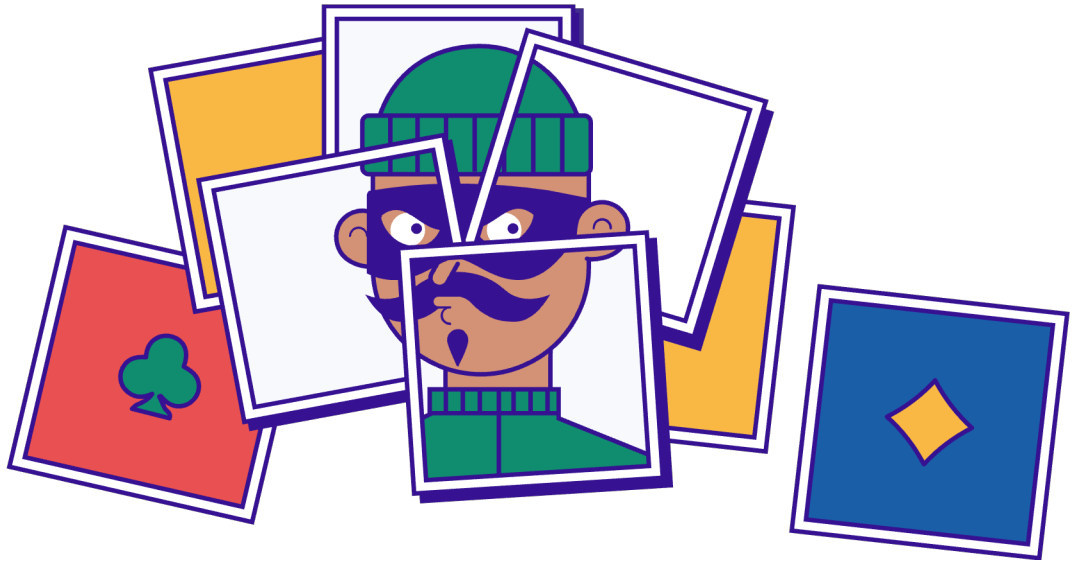
Page size
100 buckets

S3_Buckets

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

$21+4(100)=421$

In Summary…

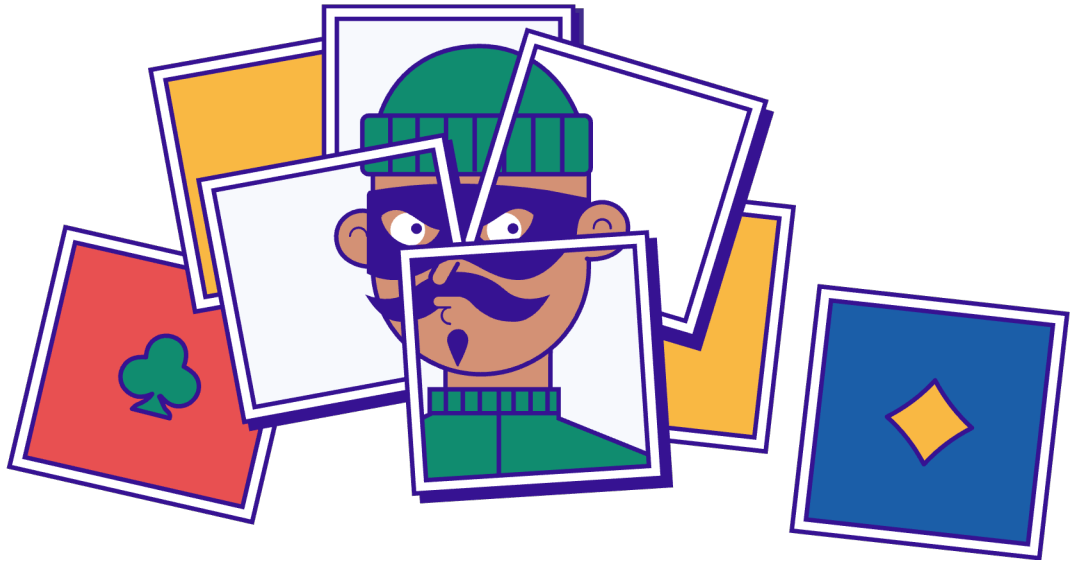


#Aggregation

In Summary...

`IAM_Users_CreateUser`

`IAM_Users`



#Aggregation

`Background_Events`

`IAM_Users_SPECIFICUSER_CreateAccessKey`

In Summary...

`IAM_Users_CreateUser`

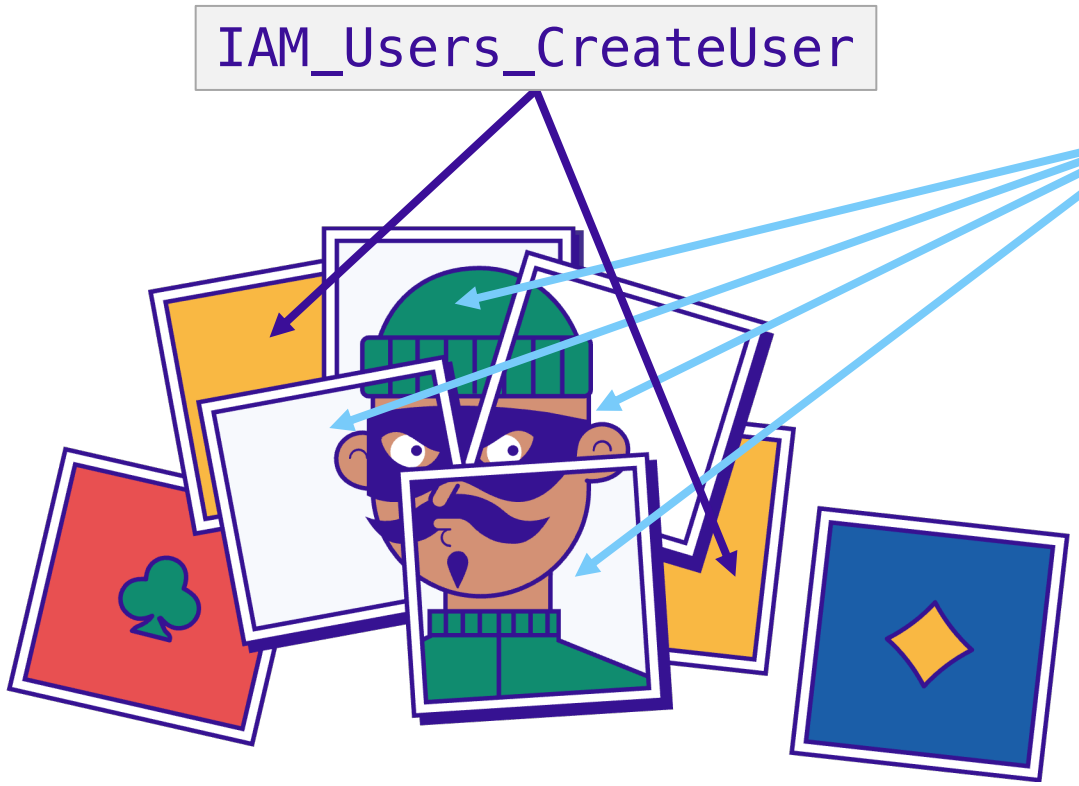
`IAM_Users`

#Aggregation

`Background_Events`

`IAM_Users_SPECIFICUSER_CreateAccessKey`

In Summary...

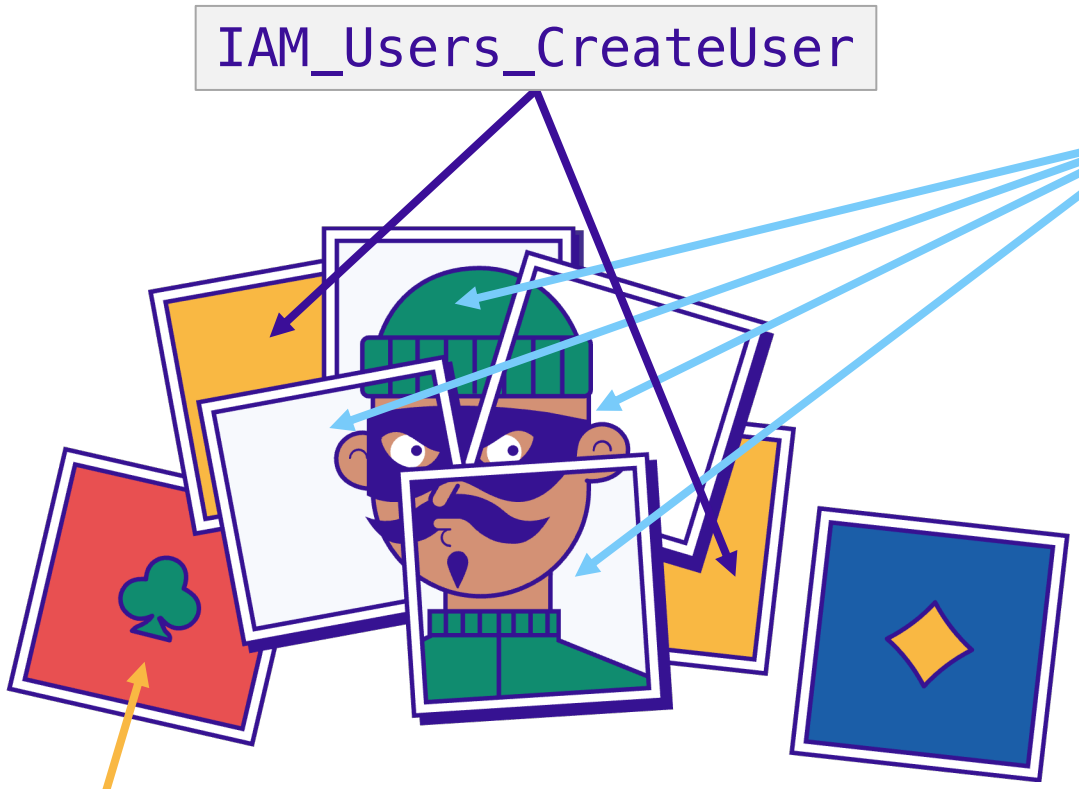


#Aggregation

Background_Events

IAM_Users_SPECIFICUSER_CreateAccessKey

In Summary...



IAM_Users_CreateUser

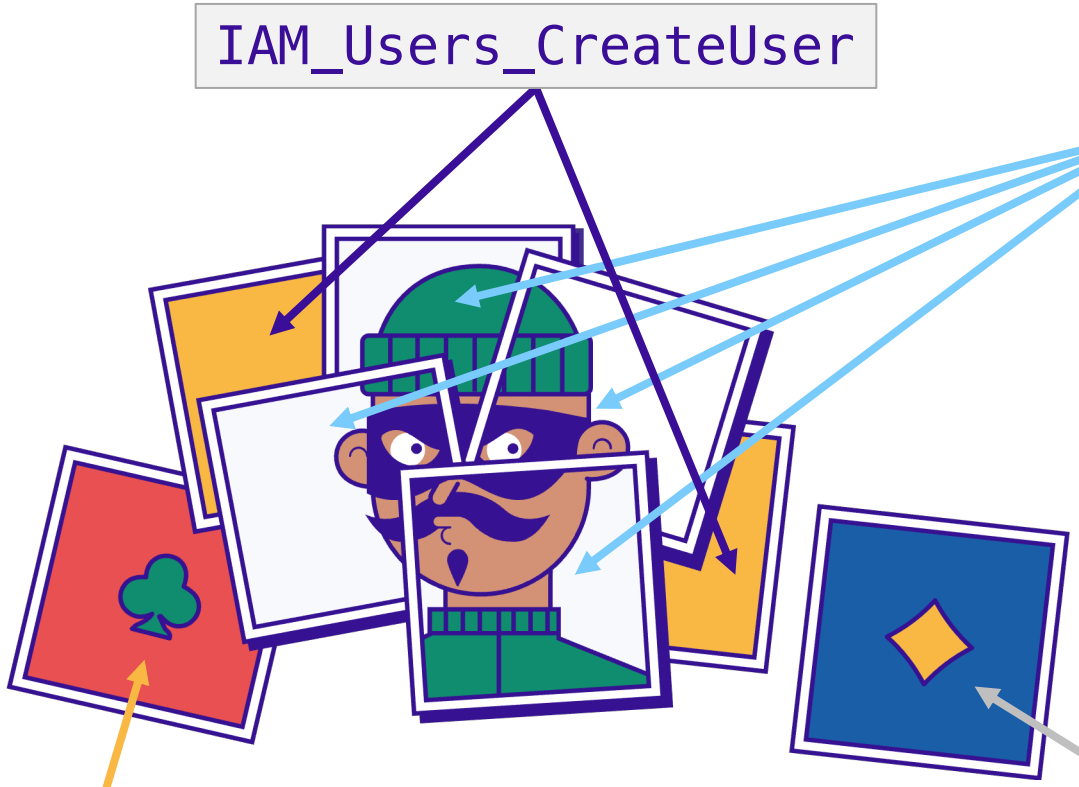
IAM_Users

#Aggregation

Background_Events

IAM_Users_SPECIFICUSER_CreateAccessKey

In Summary...



IAM_Users_CreateUser

IAM_Users

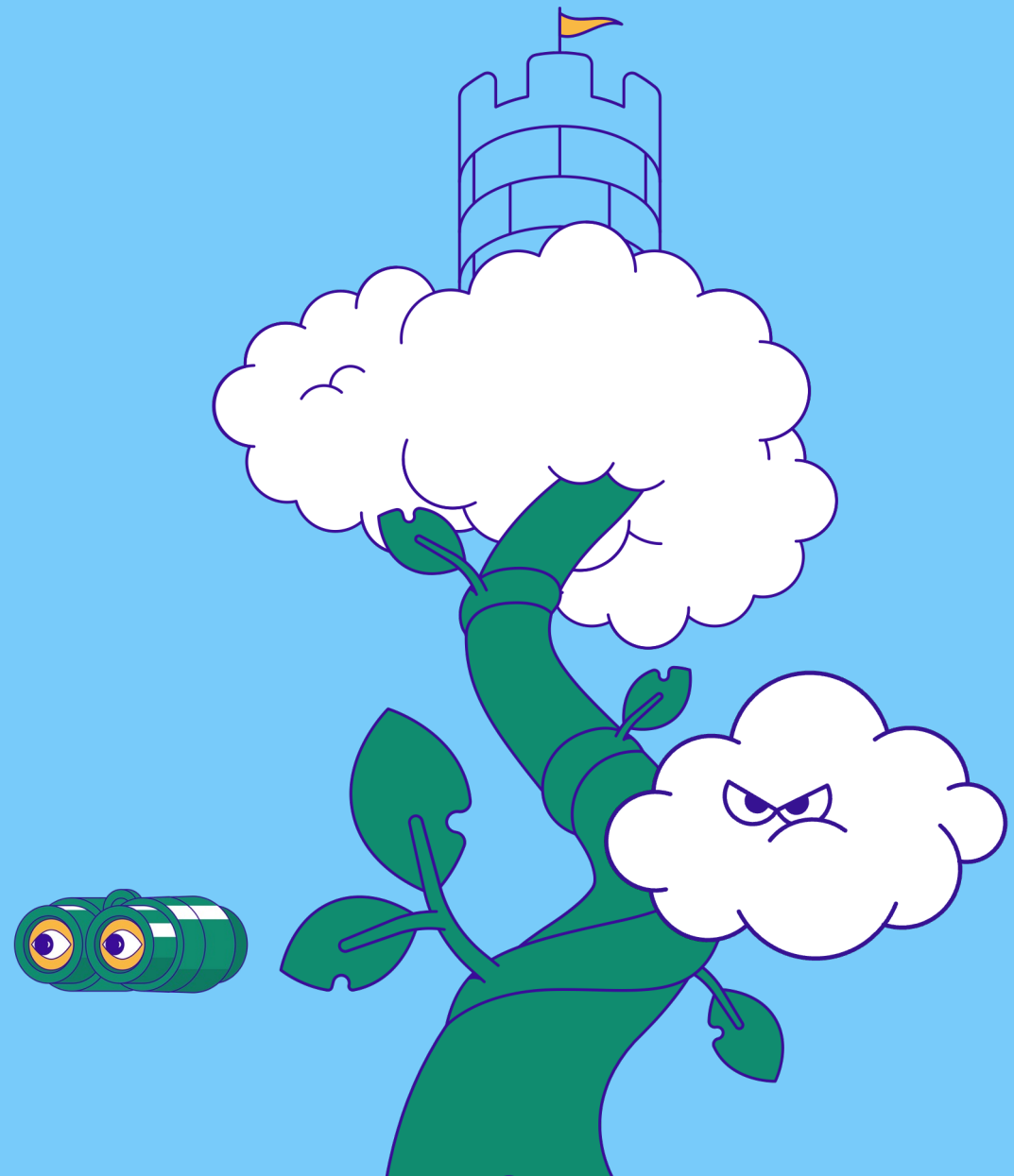
#Aggregation

Background_Events

IAM_Users_SPECIFICUSER_CreateAccessKey

AGENDA

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



2-Pass Approach – Labels + Signals

iam:ListUsers

iam:GetLoginProfile

iam:ListSigningCertificates

iam:ListMFADevices

iam:ListGroupsForUser

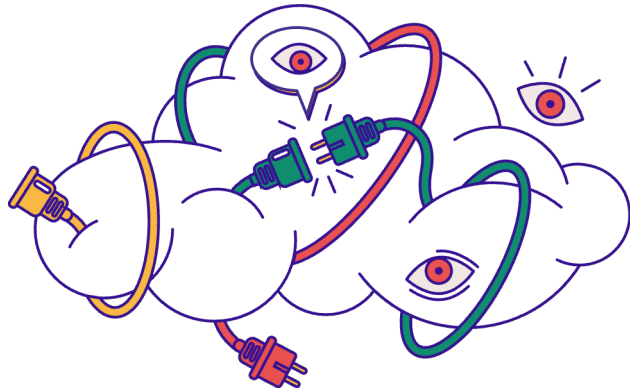
iam:ListAccessKeys

iam:GetAccessKeyLastUsed

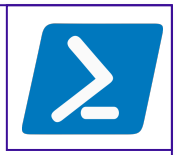
`$this.AnchorEvents`

`$this.RequiredEvents`

`$this.OptionalEvents`



Signal Definition



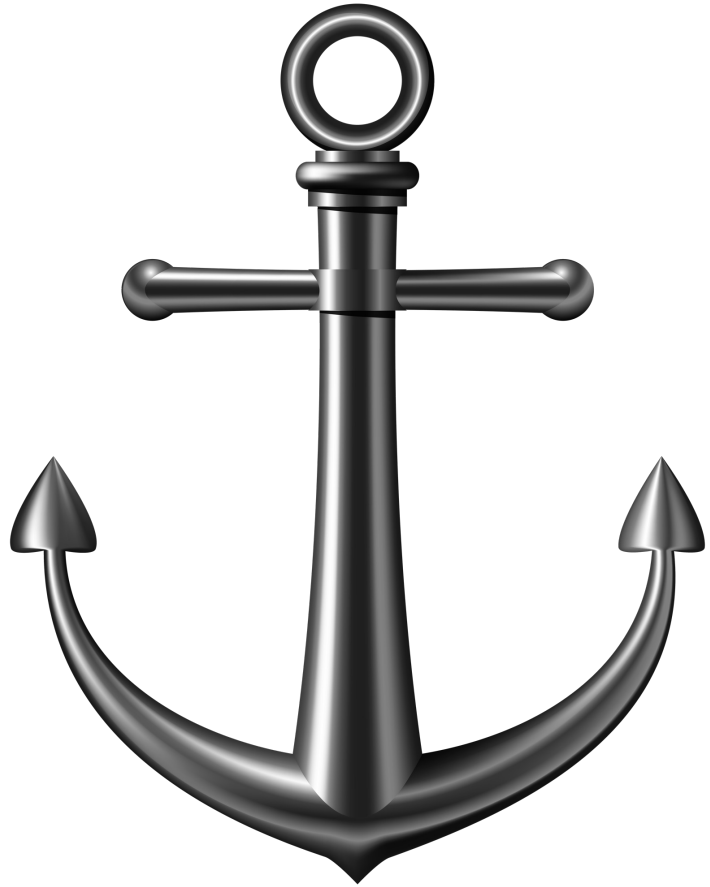
```
([LabelType]::IAM_Users) {
    $this.Service = 'IAM'
    $this.Name = 'Clicked IAM->Users'
    $this.Summary = 'Clicked IAM->Users which displays all IAM Users in paged format.'
    $this.Url = 'https://{{awsRegion}}.console.aws.amazon.com/iamv2/home?region={{awsRegion}}#/users'
    $this.AnchorEvents = @('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

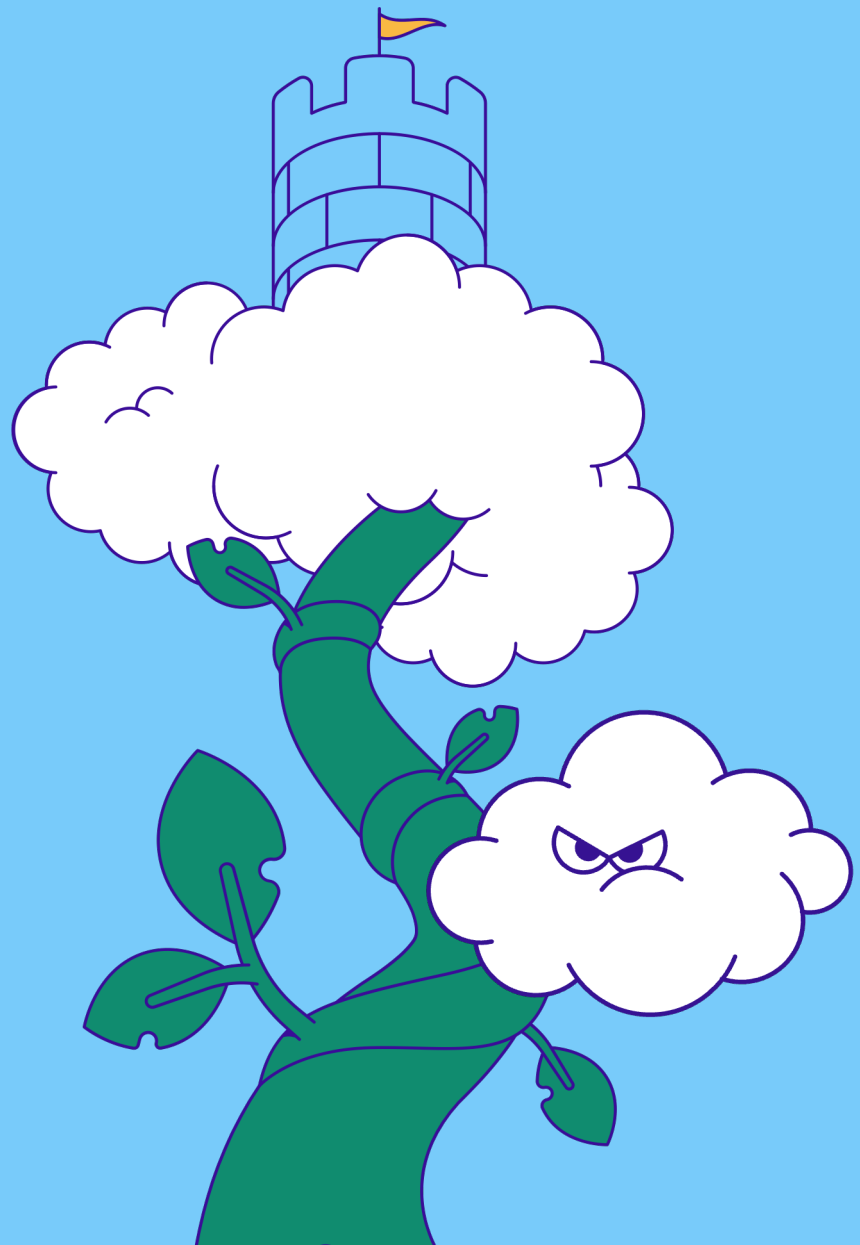


Add'l Cool Tricks & Capabilities

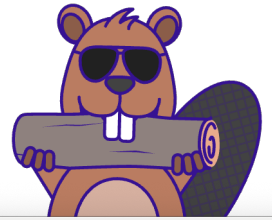
- Modification of Signal names, summaries & URLs based on data extracted from all related events
- Each Signal contains dictionary of extracted data
- Signal lookback scenarios for:
  - Modifying previous Signals
  - Changing Label for current Signal
  - Merging previous Signals
  - Extracting data from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

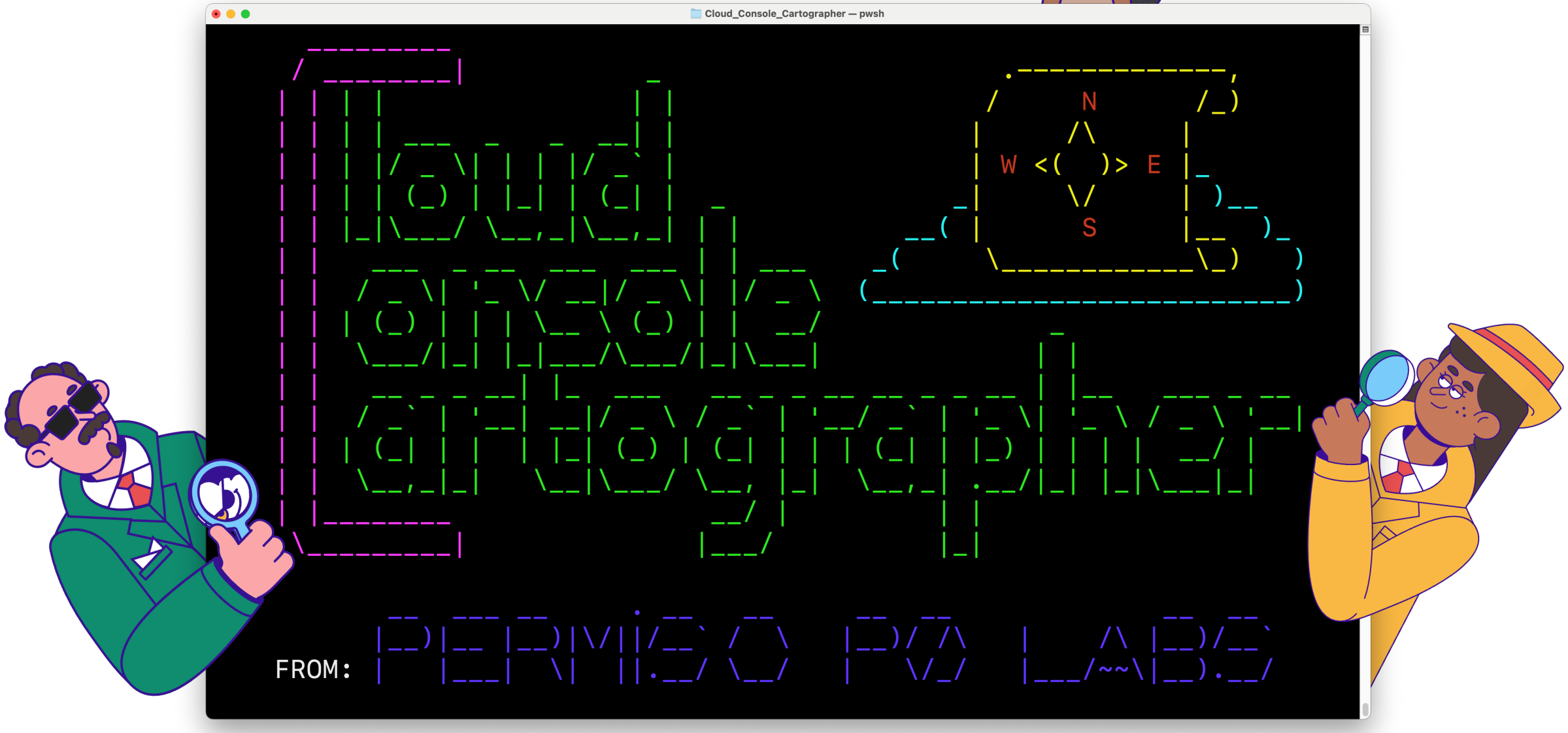
AGENDA

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



DEMO + Public Tool Release

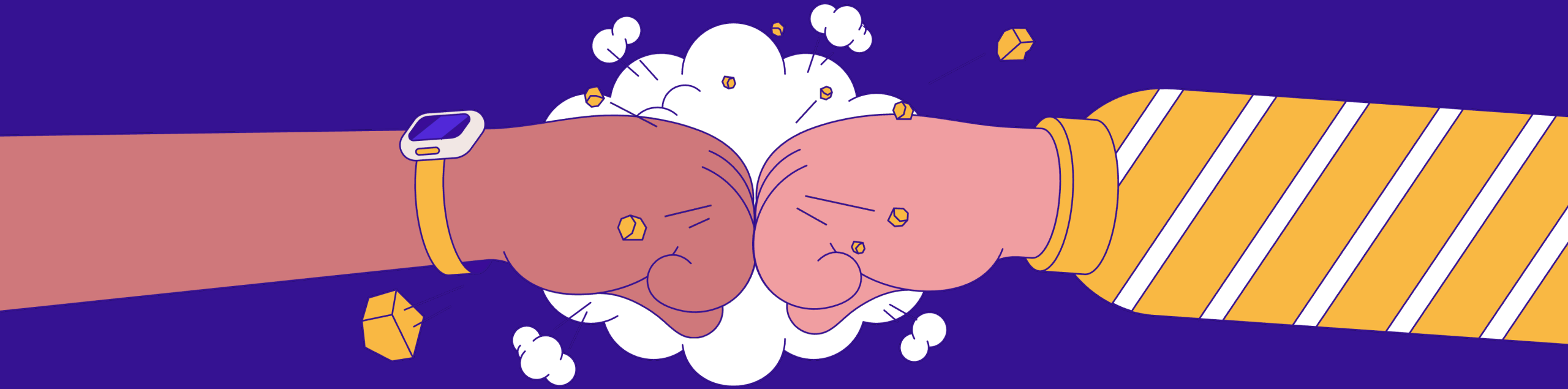


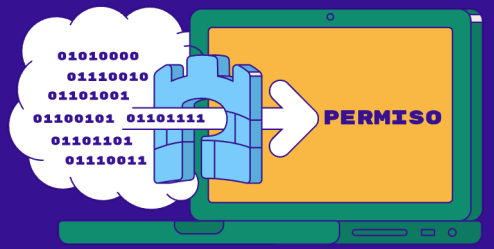


Black Hat Sound Bytes

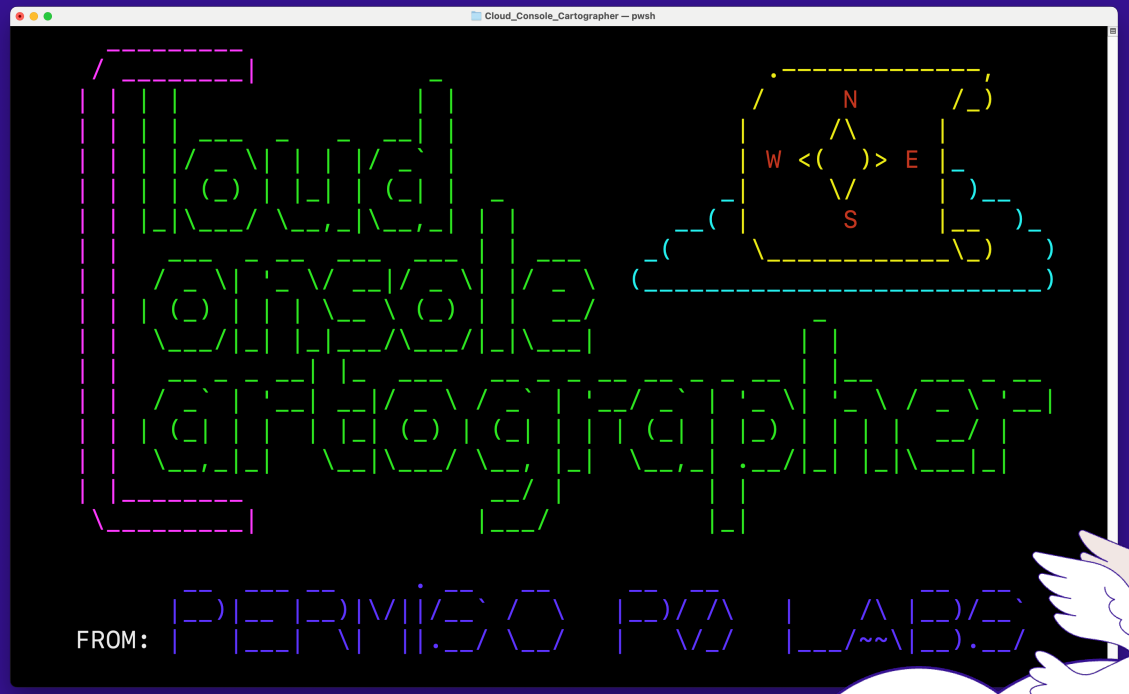
1. **Threat actors continue to use interactive console UIs** (instead of CLIs) throughout many stages of the attack lifecycle
2. **Configure the necessary cloud logging options** for retention, forwarding & querying capabilities required to detect & analyze suspicious console session logs
3. **Use Cloud 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

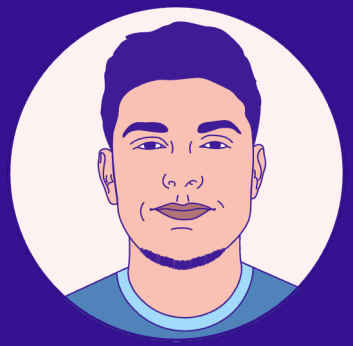
THANKS FOR YOUR TIME!





PERMISO





ANDI AHMETI

andi-ahmeti

@SecEagleAnd1

DANIEL BOHANNON

danielhbohannon

@danielhbohannon

https://github.com/Permiso-io-tools/**CloudConsoleCartographer**