THE PHANTOM OF THE INFRASTRUCTURE

Investigating the Hidden IAM Risks in Bedrock API Keys



SERGIO GARCIA

- Security Researcher @ BeyondTrust Phantom Labs™
- Former Founding Engineer @ Prowler
- Based in Miami, originally from Spain
- I break things in AWS so you don't have to
- Twitter/GitHub/LinkedIn: @MrCloudSec



Accelerate AI development with Amazon Bedrock API keys

by Sofian Hamiti, Ajit Mahareddy, Massimiliano Angelino, Huong Nguyen, and Nakul Vankadari Ramesh | on 08 JUL 2025 | in Amazon Bedrock, Amazon Machine Learning, Announcements, Artificial Intelligence, Foundation models | Permalink | Comments | Share

Today, we're excited to announce a significant improvement to the developer experience of Amazon Bedrock: API keys. API keys provide a new way to access the Amazon Bedrock APIs, streamlining the authentication process so that developers can focus on building rather than configuration.

AGENDA

- How Bedrock API Keys work
- Decoding the keys
- Attack scenarios
- How to detect this
- How to not get wrecked

UNDERSTANDING BEDROCK API KEYS

WHAT ARE BEDROCK API KEYS?

```
export AWS_BEARER_TOKEN_BEDROCK=${api-key}
```

July 2025

AWS launches Bedrock API keys

- "Simplify AI development"
- Alternative to AWS credentials

3 ways to use them:

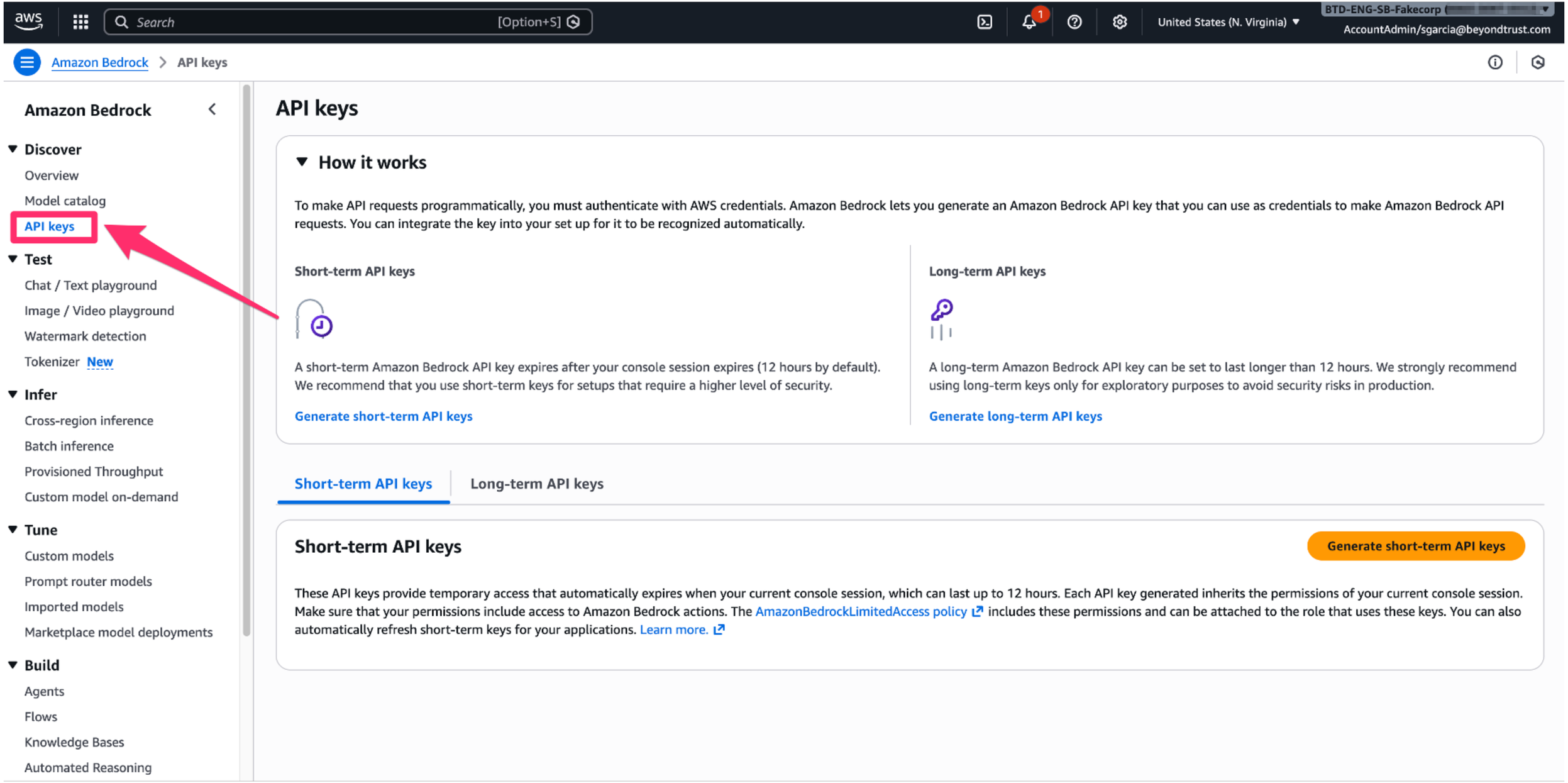
- AWS CLI (export as env vars)
- AWS SDKs (export as env vars)
- Direct HTTP requests (bearer token in header)

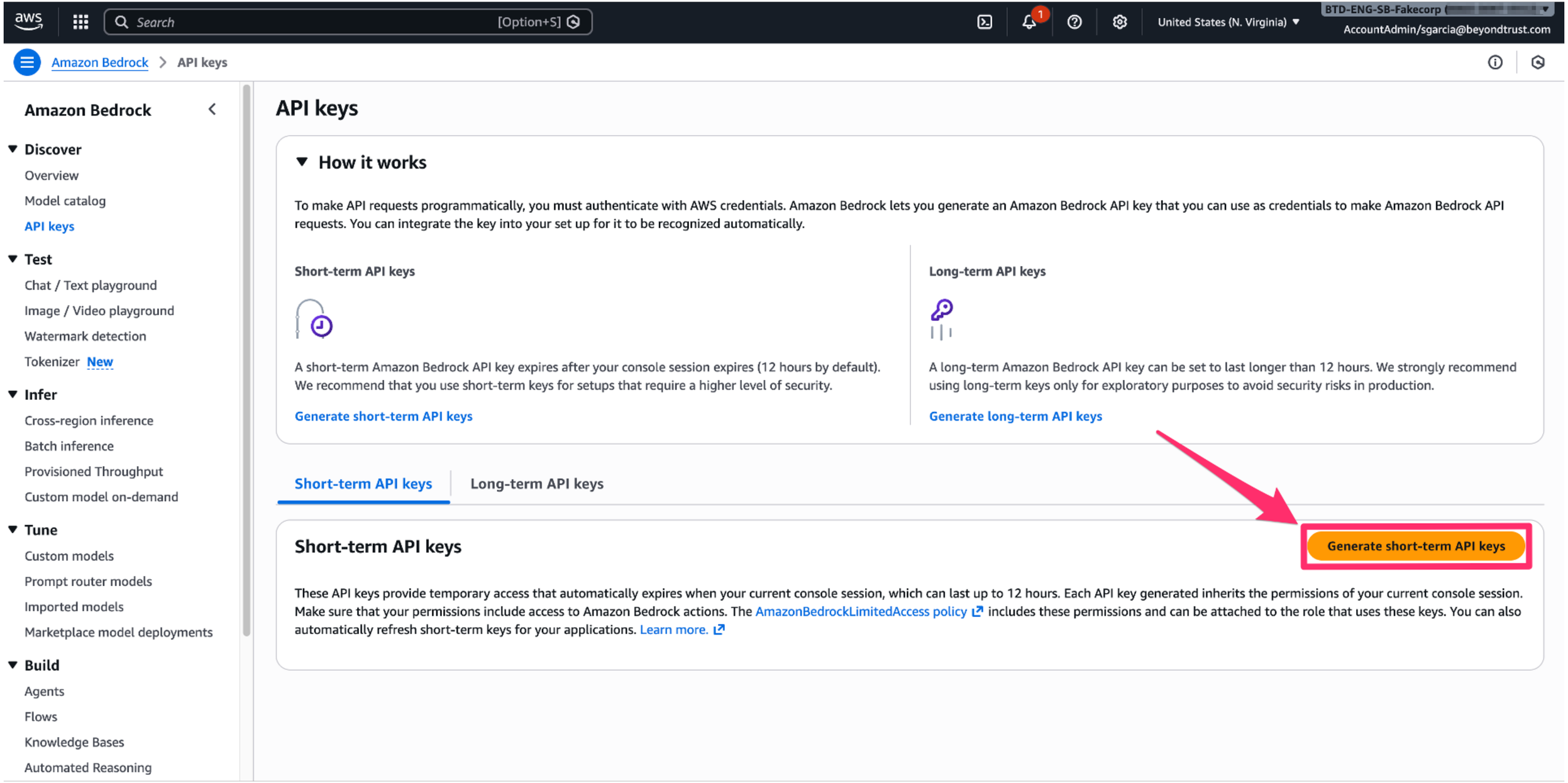
```
Authorization: Bearer $AWS_BEARER_TOKEN_BEDROCK
```

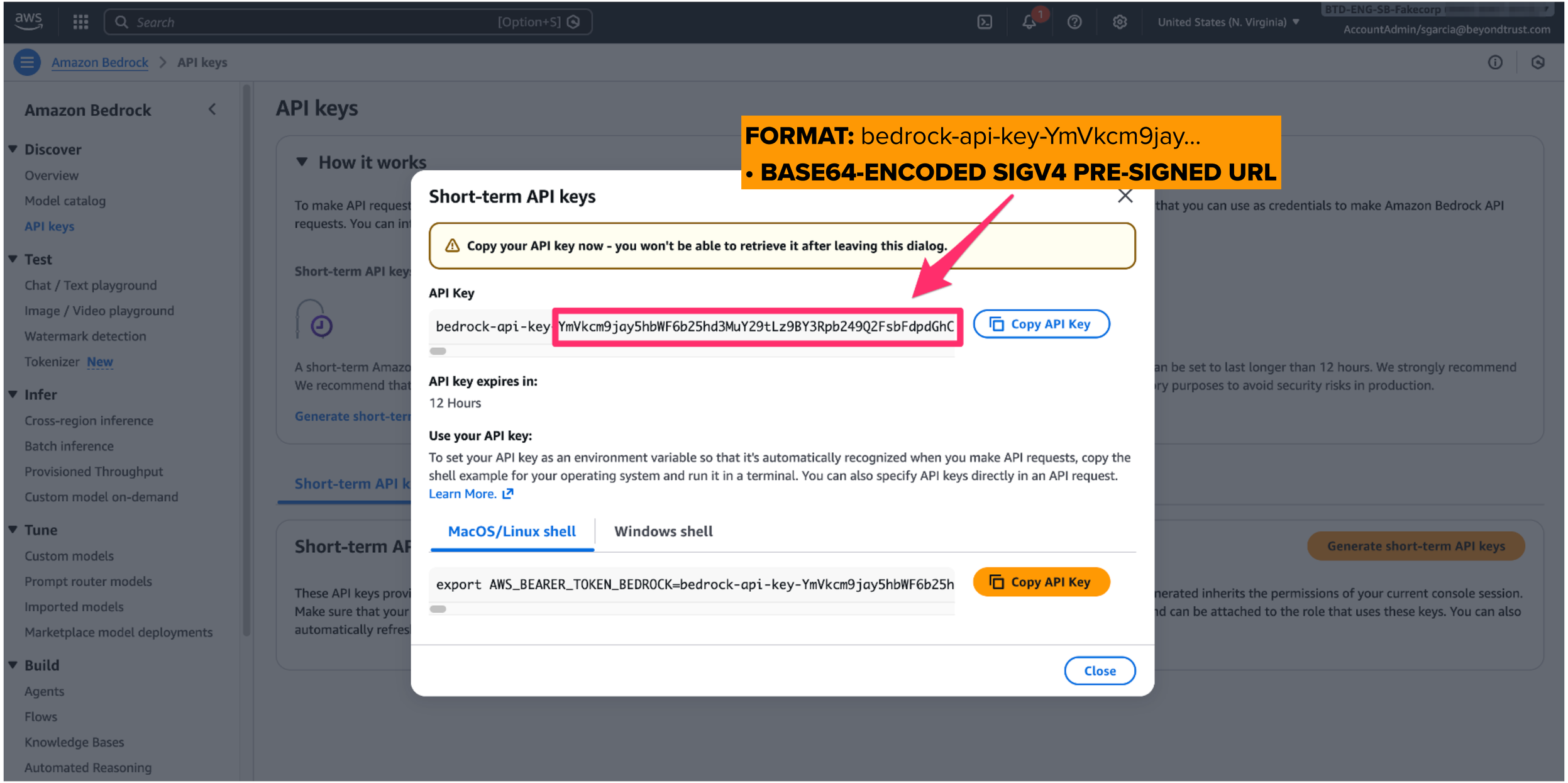
Two types:

- Short-term
- Long-term (riskier)

14 DAYS LATER: Keys appear on public GitHub


aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
API keys
How it works
To make API requests programmatically, you must authenticate with AWS credentials. Amazon Bedrock lets you generate an Amazon Bedrock API key that you can use as credentials to make Amazon Bedrock API requests. You can integrate the key into your set up for it to be recognized automatically.
Short-term API keys
A short-term Amazon Bedrock API key expires after your console session expires (12 hours by default). We recommend that you use short-term keys for setups that require a higher level of security.
Generate short-term API keys
Long-term API keys
A long-term Amazon Bedrock API key can be set to last longer than 12 hours. We strongly recommend using long-term keys only for exploratory purposes to avoid security risks in production.
Generate long-term API keys
Short-term API keys
Long-term API keys
Short-term API keys
Generate short-term API keys
These API keys provide temporary access that automatically expires when your current console session, which can last up to 12 hours. Each API key generated inherits the permissions of your current console session. Make sure that your permissions include access to Amazon Bedrock actions. The AmazonBedrockLimitedAccess policy includes these permissions and can be attached to the role that uses these keys. You can also automatically refresh short-term keys for your applications. Learn more.


aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
API keys
How it works
To make API requests programmatically, you must authenticate with AWS credentials. Amazon Bedrock lets you generate an Amazon Bedrock API key that you can use as credentials to make Amazon Bedrock API requests. You can integrate the key into your set up for it to be recognized automatically.
Short-term API keys
A short-term Amazon Bedrock API key expires after your console session expires (12 hours by default). We recommend that you use short-term keys for setups that require a higher level of security.
Generate short-term API keys
Long-term API keys
A long-term Amazon Bedrock API key can be set to last longer than 12 hours. We strongly recommend using long-term keys only for exploratory purposes to avoid security risks in production.
Generate long-term API keys
Short-term API keys
Long-term API keys
Short-term API keys
Generate short-term API keys
These API keys provide temporary access that automatically expires when your current console session, which can last up to 12 hours. Each API key generated inherits the permissions of your current console session. Make sure that your permissions include access to Amazon Bedrock actions. The AmazonBedrockLimitedAccess policy includes these permissions and can be attached to the role that uses these keys. You can also automatically refresh short-term keys for your applications. Learn more.


FORMAT: bedrock-api-key-YmVkcm9jay...
• BASE64-ENCODED SIGV4 PRE-SIGNED URL
Short-term API keys
Copy your API key now - you won't be able to retrieve it after leaving this dialog.
API Key
bedrock-api-key-YmVkcm9jay5hbWF6b25hd3MuY29tLz9BY3Rpb249Q2FsbFdpdGhC
Copy API Key
API key expires in:
12 Hours
Use your API key:
To set your API key as an environment variable so that it's automatically recognized when you make API requests, copy the shell example for your operating system and run it in a terminal. You can also specify API keys directly in an API request.
Learn More.
MacOS/Linux shell
Windows shell
export AWS_BEARER_TOKEN_BEDROCK=bedrock-api-key-YmVkcm9jay5hbWF6b25h
Copy API Key
Close

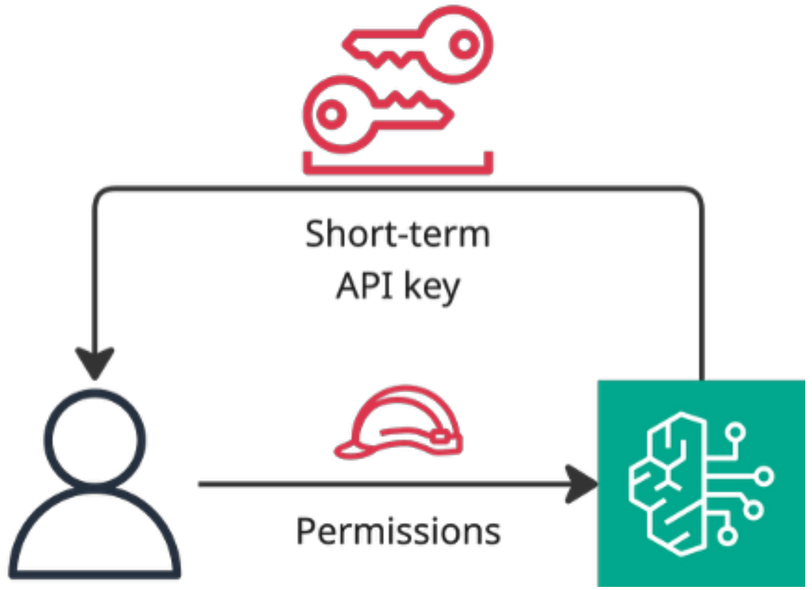
SHORT-TERM KEYS

No identity is created: uses YOUR existing session

- Inherits ALL your permissions (but only usable in Bedrock)
- Expires with session up to 12 hours

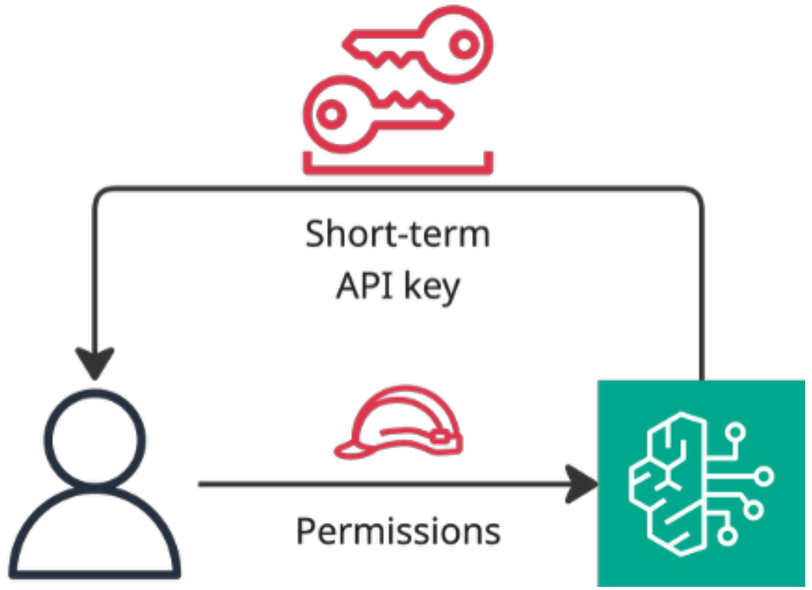
Creation Happens client-side

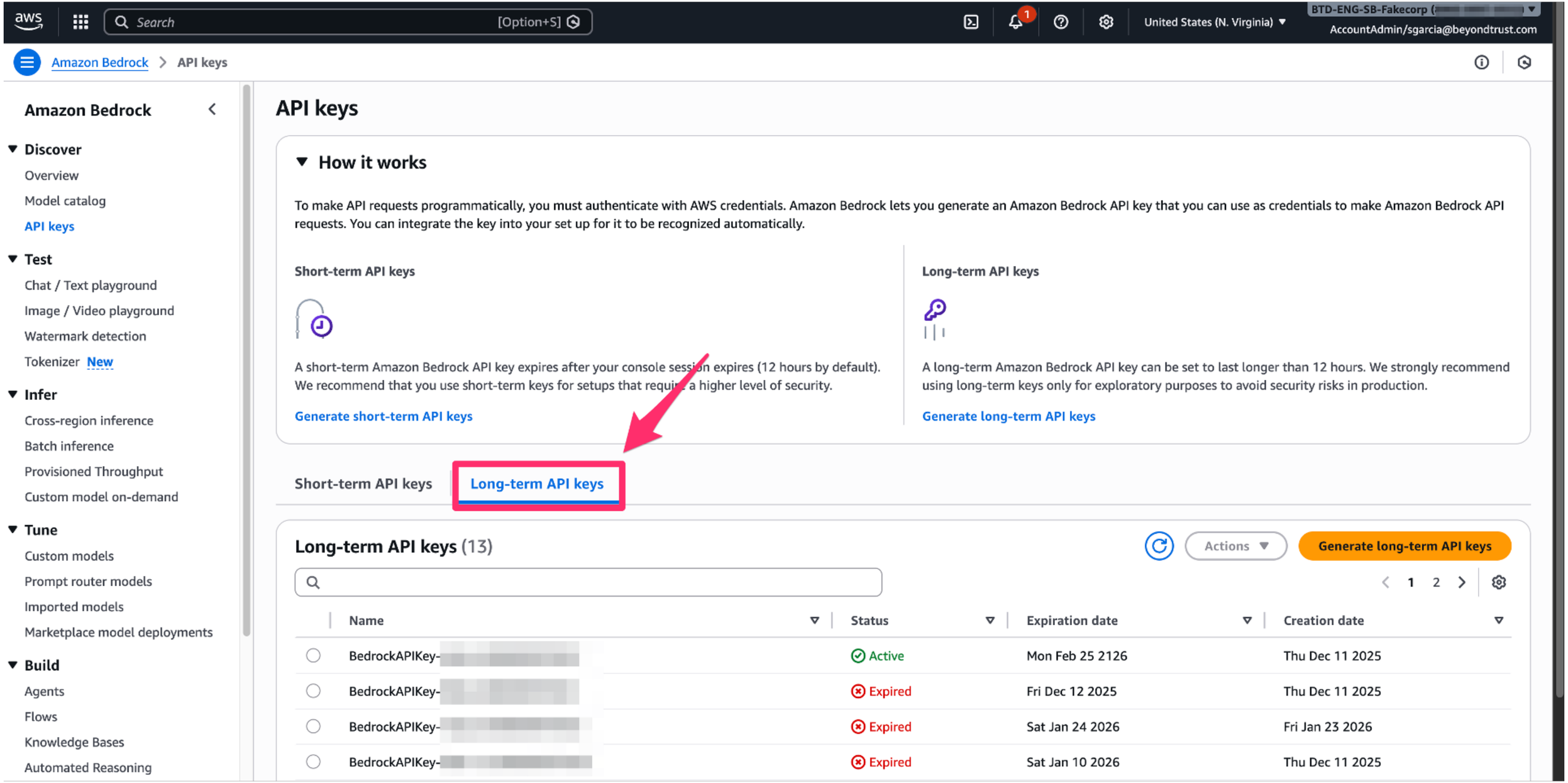
- No CloudTrail event for creation! (only when used)

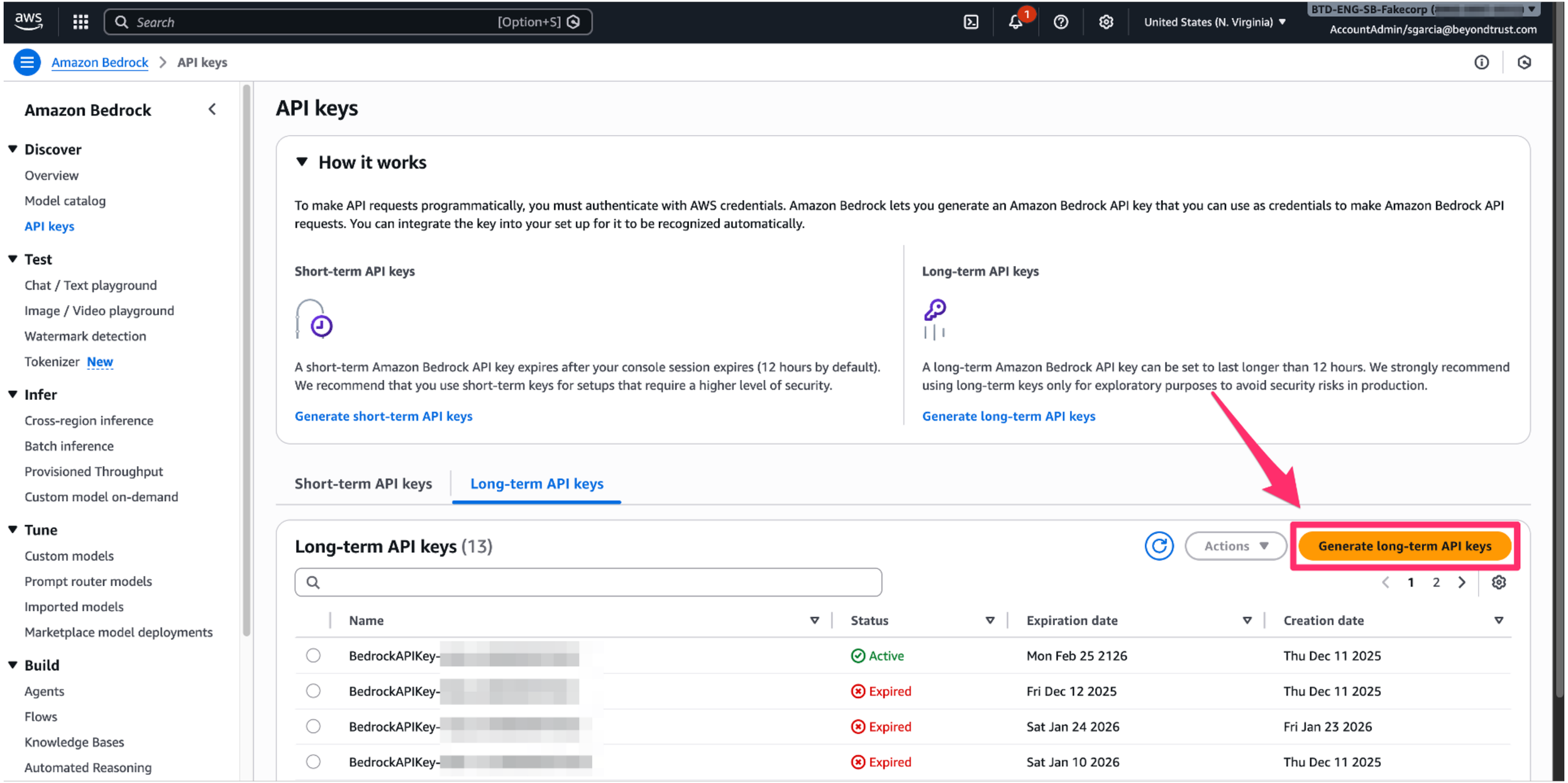


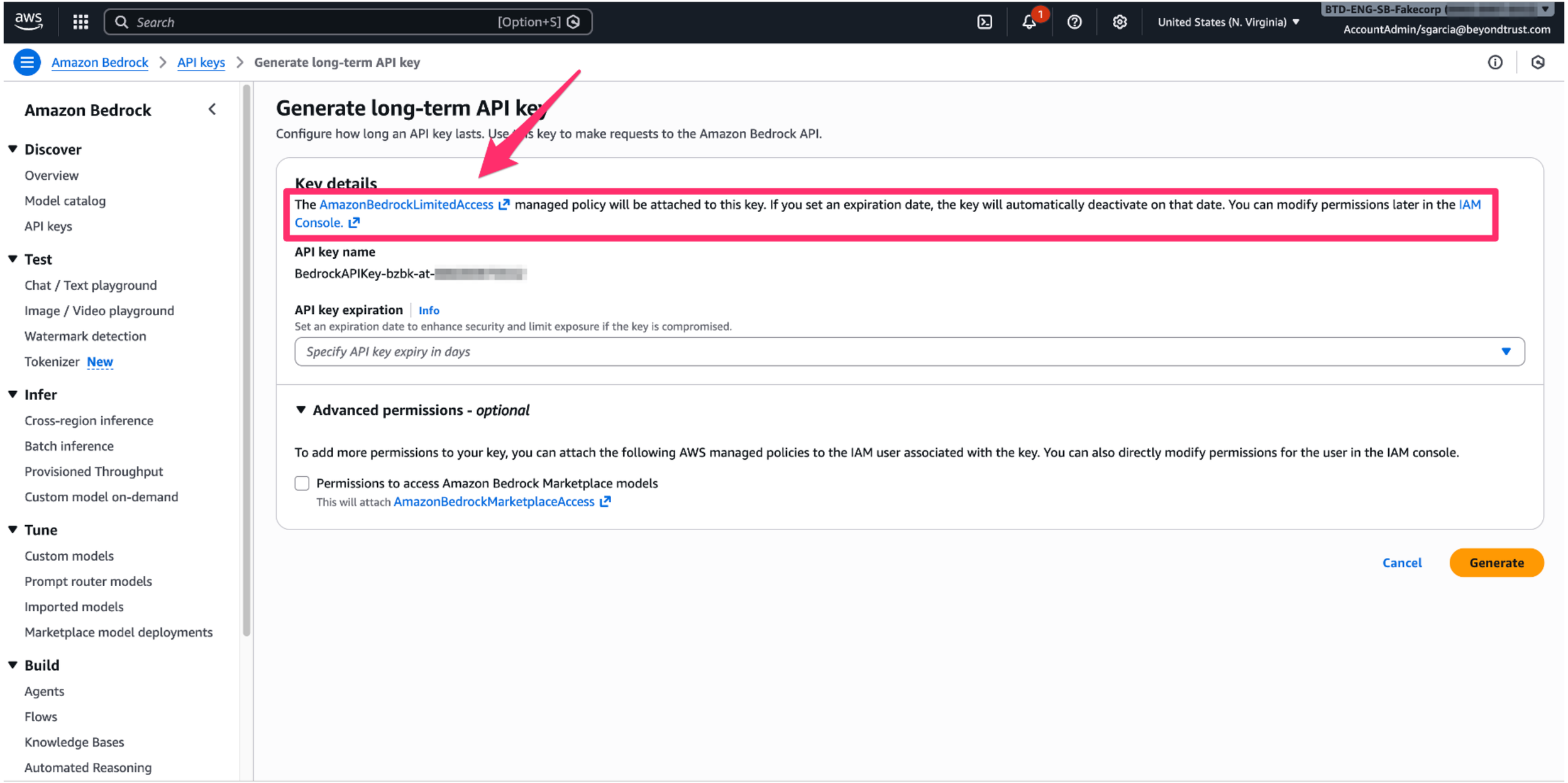
SHORT-TERM KEYS

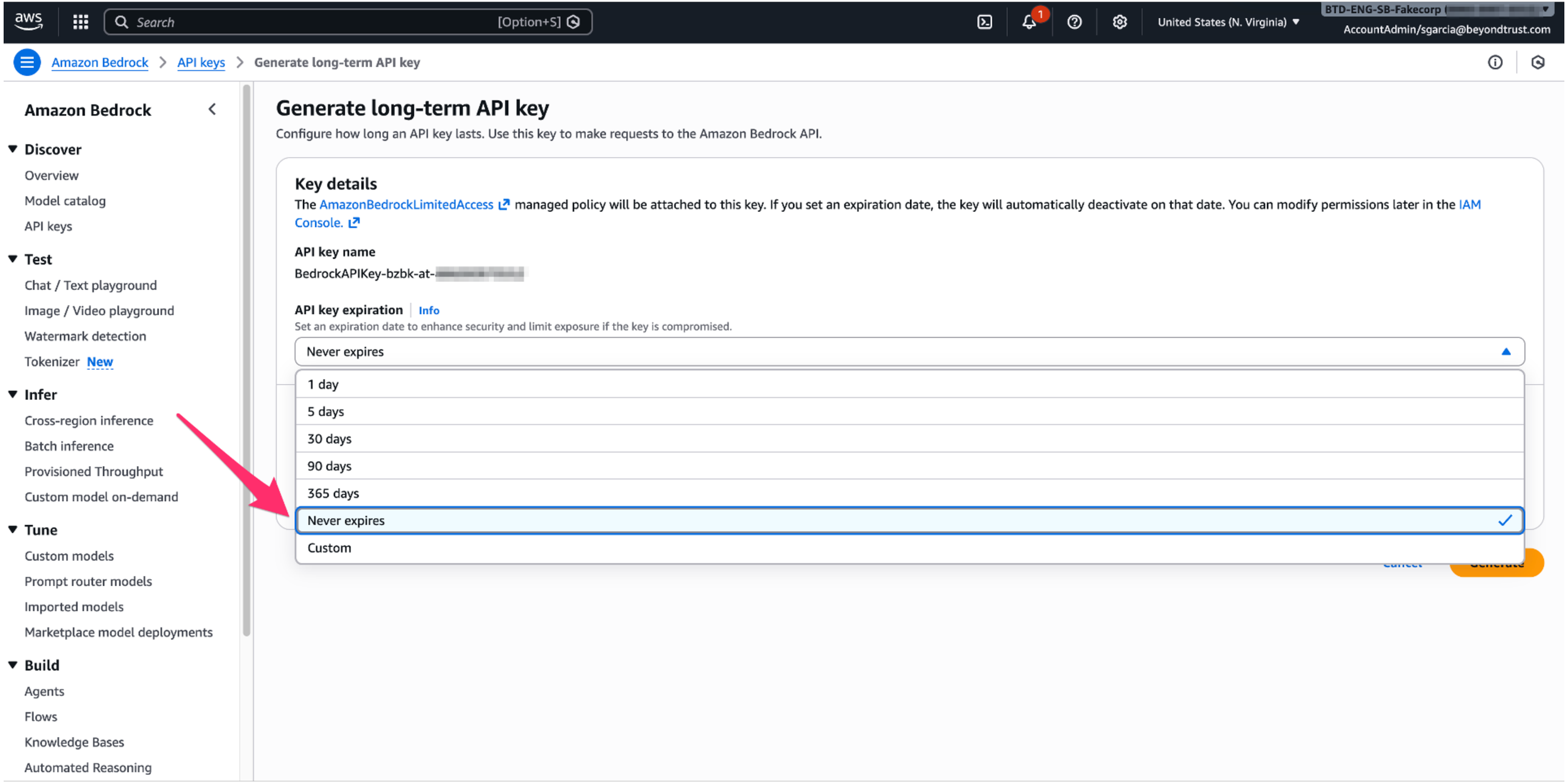
```
{
  "service": "bedrock",
  "region": "us-east-1",
  "method": "POST",
  "path": "/",
  "protocol": "https",
  "hostname": "bedrock.amazonaws.com",
  "headers": {
    "host": "bedrock.amazonaws.com",
    "authorization": "AWS4-HMAC-SHA256 Credential=PLACEHOLDER
      /20240726/us-east-1/bedrock/aws4_request, SignedHeaders
      =host;"
  },
  "query": {
    "Action": "CallWithBearerToken"
  }
}
```

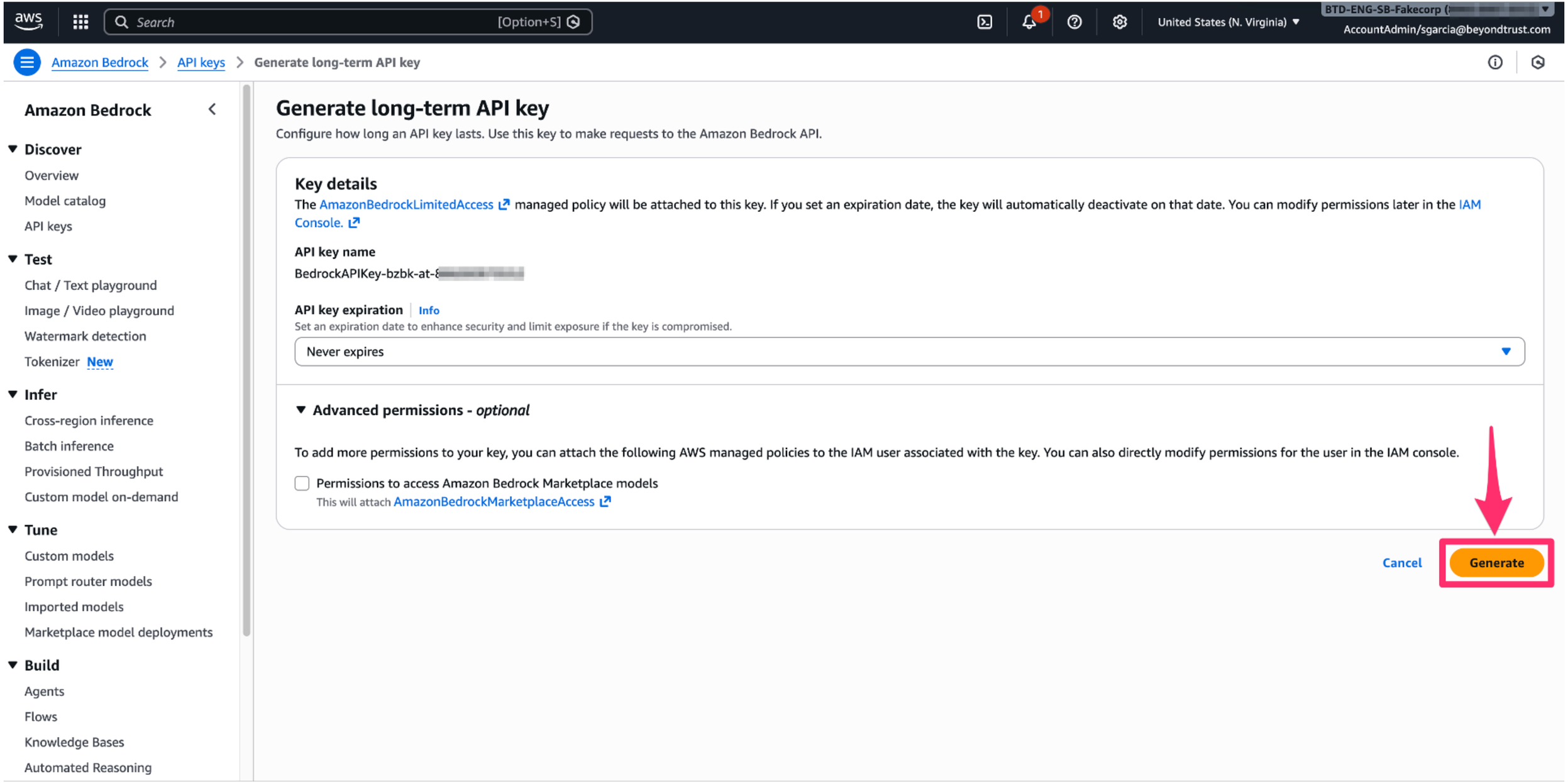


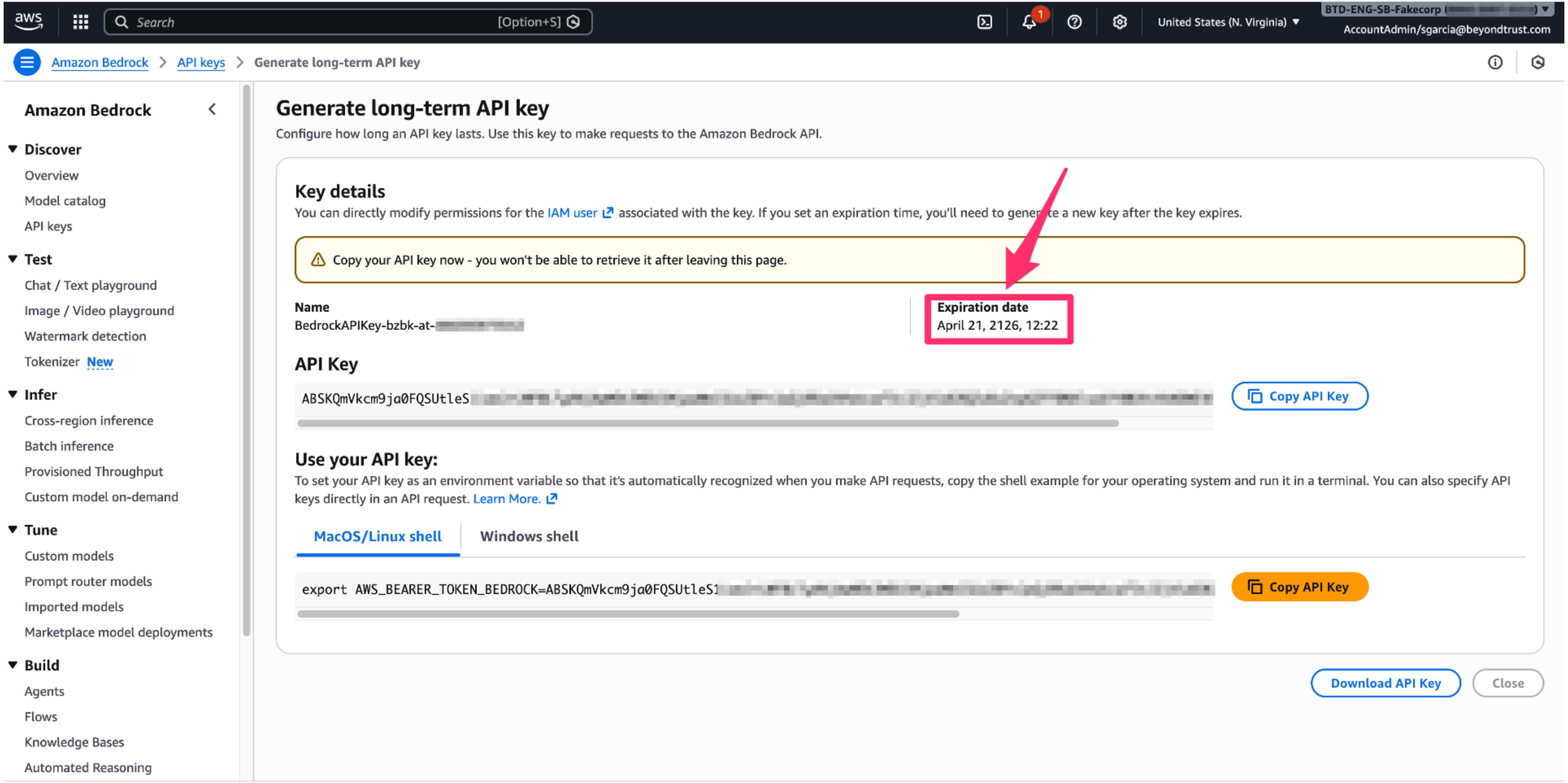

aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
API keys
How it works
To make API requests programmatically, you must authenticate with AWS credentials. Amazon Bedrock lets you generate an Amazon Bedrock API key that you can use as credentials to make Amazon Bedrock API requests. You can integrate the key into your set up for it to be recognized automatically.
Short-term API keys
A short-term Amazon Bedrock API key expires after your console session expires (12 hours by default). We recommend that you use short-term keys for setups that require a higher level of security.
Generate short-term API keys
Long-term API keys
A long-term Amazon Bedrock API key can be set to last longer than 12 hours. We strongly recommend using long-term keys only for exploratory purposes to avoid security risks in production.
Generate long-term API keys
Short-term API keys
Long-term API keys
Long-term API keys (13)
Actions
Generate long-term API keys
1
2
Name
Status
Expiration date
Creation date
BedrockAPIKey-
Active
Mon Feb 25 2126
Thu Dec 11 2025
BedrockAPIKey-
Expired
Fri Dec 12 2025
Thu Dec 11 2025
BedrockAPIKey-
Expired
Sat Jan 24 2026
Fri Jan 23 2026
BedrockAPIKey-
Expired
Sat Jan 10 2026
Thu Dec 11 2025

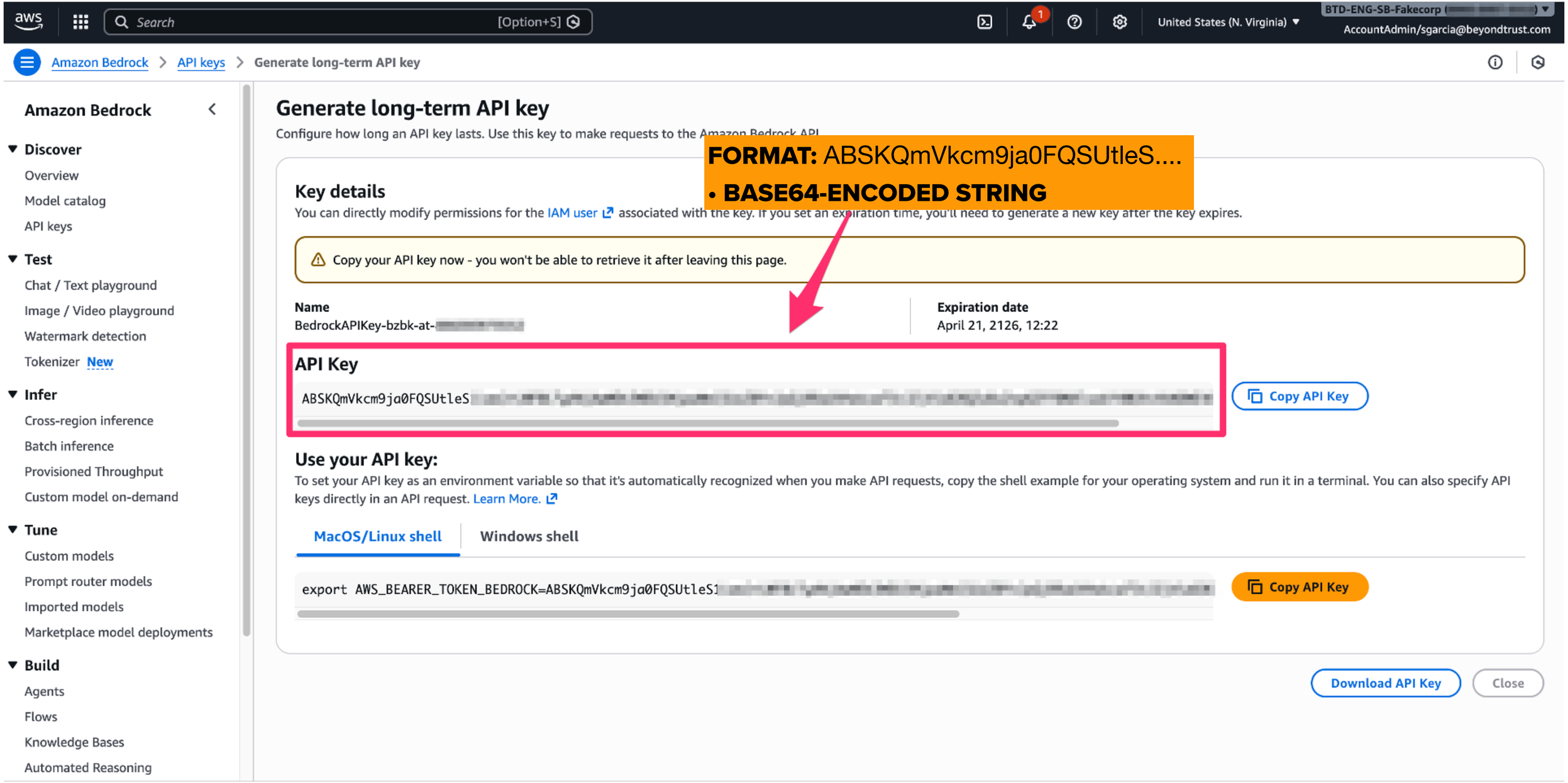

Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
API keys
How it works
To make API requests programmatically, you must authenticate with AWS credentials. Amazon Bedrock lets you generate an Amazon Bedrock API key that you can use as credentials to make Amazon Bedrock API requests. You can integrate the key into your set up for it to be recognized automatically.
Short-term API keys
A short-term Amazon Bedrock API key expires after your console session expires (12 hours by default). We recommend that you use short-term keys for setups that require a higher level of security.
Generate short-term API keys
Long-term API keys
A long-term Amazon Bedrock API key can be set to last longer than 12 hours. We strongly recommend using long-term keys only for exploratory purposes to avoid security risks in production.
Generate long-term API keys
Short-term API keys
Long-term API keys
Long-term API keys (13)
Actions
Generate long-term API keys
1
2
Name
Status
Expiration date
Creation date
BedrockAPIKey-
Active
Mon Feb 25 2126
Thu Dec 11 2025
BedrockAPIKey-
Expired
Fri Dec 12 2025
Thu Dec 11 2025
BedrockAPIKey-
Expired
Sat Jan 24 2026
Fri Jan 23 2026
BedrockAPIKey-
Expired
Sat Jan 10 2026
Thu Dec 11 2025


aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Generate long-term API key
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
Generate long-term API key
Configure how long an API key lasts. Use this key to make requests to the Amazon Bedrock API.
Key details
The AmazonBedrockLimitedAccess managed policy will be attached to this key. If you set an expiration date, the key will automatically deactivate on that date. You can modify permissions later in the IAM Console.
API key name
BedrockAPIKey-bzbk-at-
API key expiration
Info
Set an expiration date to enhance security and limit exposure if the key is compromised.
Specify API key expiry in days
Advanced permissions - optional
To add more permissions to your key, you can attach the following AWS managed policies to the IAM user associated with the key. You can also directly modify permissions for the user in the IAM console.
Permissions to access Amazon Bedrock Marketplace models
This will attach AmazonBedrockMarketplaceAccess
Cancel
Generate

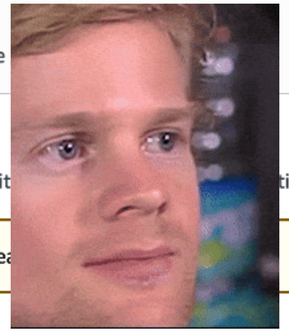

Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Generate long-term API key
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
Generate long-term API key
Configure how long an API key lasts. Use this key to make requests to the Amazon Bedrock API.
Key details
The AmazonBedrockLimitedAccess managed policy will be attached to this key. If you set an expiration date, the key will automatically deactivate on that date. You can modify permissions later in the IAM Console.
API key name
BedrockAPIKey-bzbk-at-
API key expiration
Info
Set an expiration date to enhance security and limit exposure if the key is compromised.
Never expires
1 day
5 days
30 days
90 days
365 days
Never expires
Custom


aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Generate long-term API key
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
Generate long-term API key
Configure how long an API key lasts. Use this key to make requests to the Amazon Bedrock API.
Key details
The AmazonBedrockLimitedAccess managed policy will be attached to this key. If you set an expiration date, the key will automatically deactivate on that date. You can modify permissions later in the IAM Console.
API key name
BedrockAPIKey-bzbk-at-
API key expiration
Info
Set an expiration date to enhance security and limit exposure if the key is compromised.
Never expires
Advanced permissions - optional
To add more permissions to your key, you can attach the following AWS managed policies to the IAM user associated with the key. You can also directly modify permissions for the user in the IAM console.
Permissions to access Amazon Bedrock Marketplace models
This will attach AmazonBedrockMarketplaceAccess
Cancel
Generate


aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Generate long-term API key
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
Generate long-term API key
Configure how long an API key lasts. Use this key to make requests to the Amazon Bedrock API.
Key details
You can directly modify permissions for the IAM user associated with the key. If you set an expiration time, you'll need to generate a new key after the key expires.
Copy your API key now - you won't be able to retrieve it after leaving this page.
Name
BedrockAPIKey-bzbk-at-
Expiration date
April 21, 2126, 12:22
API Key
ABSKQmVkcm9ja0FQSUtleS
Copy API Key
Use your API key:
To set your API key as an environment variable so that it's automatically recognized when you make API requests, copy the shell example for your operating system and run it in a terminal. You can also specify API keys directly in an API request. Learn More.
MacOS/Linux shell
Windows shell
export AWS_BEARER_TOKEN_BEDROCK=ABSKQmVkcm9ja0FQSUtleS1
Copy API Key
Download API Key
Close


aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
Amazon Bedrock
API keys
Generate long-term API key
Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning
Generate long-term API key
Configure how long an API key lasts. Use this key to make requests to the Amazon Bedrock API
FORMAT: ABSKQmVkcm9ja0FQSUtleS....
• BASE64-ENCODED STRING
Key details
You can directly modify permissions for the IAM user associated with the key. If you set an expiration time, you'll need to generate a new key after the key expires.
Copy your API key now - you won't be able to retrieve it after leaving this page.
Name
BedrockAPIKey-bzbk-at-
Expiration date
April 21, 2126, 12:22
API Key
ABSKQmVkcm9ja0FQSUtleS
Copy API Key
Use your API key:
To set your API key as an environment variable so that it's automatically recognized when you make API requests, copy the shell example for your operating system and run it in a terminal. You can also specify API keys directly in an API request. Learn More.
MacOS/Linux shell
Windows shell
export AWS_BEARER_TOKEN_BEDROCK=ABSKQmVkcm9ja0FQSUtleS1
Copy API Key
Download API Key
Close

AN IAM USER WAS CREATED ?!



Amazon Bedrock
Discover
Overview
Model catalog
API keys
Test
Chat / Text playground
Image / Video playground
Watermark detection
Tokenizer New
Infer
Cross-region inference
Batch inference
Provisioned Throughput
Custom model on-demand
Tune
Custom models
Prompt router models
Imported models
Marketplace model deployments
Build
Agents
Flows
Knowledge Bases
Automated Reasoning

Generate long-term API key

Configure how long an API key lasts. Use this key to make requests to the

Key details

You can directly modify permissions for the IAM user associated with it. tion time, you'll need to generate a new key after the key expires.

⚠ Copy your API key now - you won't be able to retrieve it after lea

Name
BedrockAPIKey-bzbk-at-[redacted]

Expiration date
April 21, 2126, 12:22

API Key

```
ABSKQmVkcm9ja0FQSUtleS[redacted]
```

Copy API Key

Use your API key:

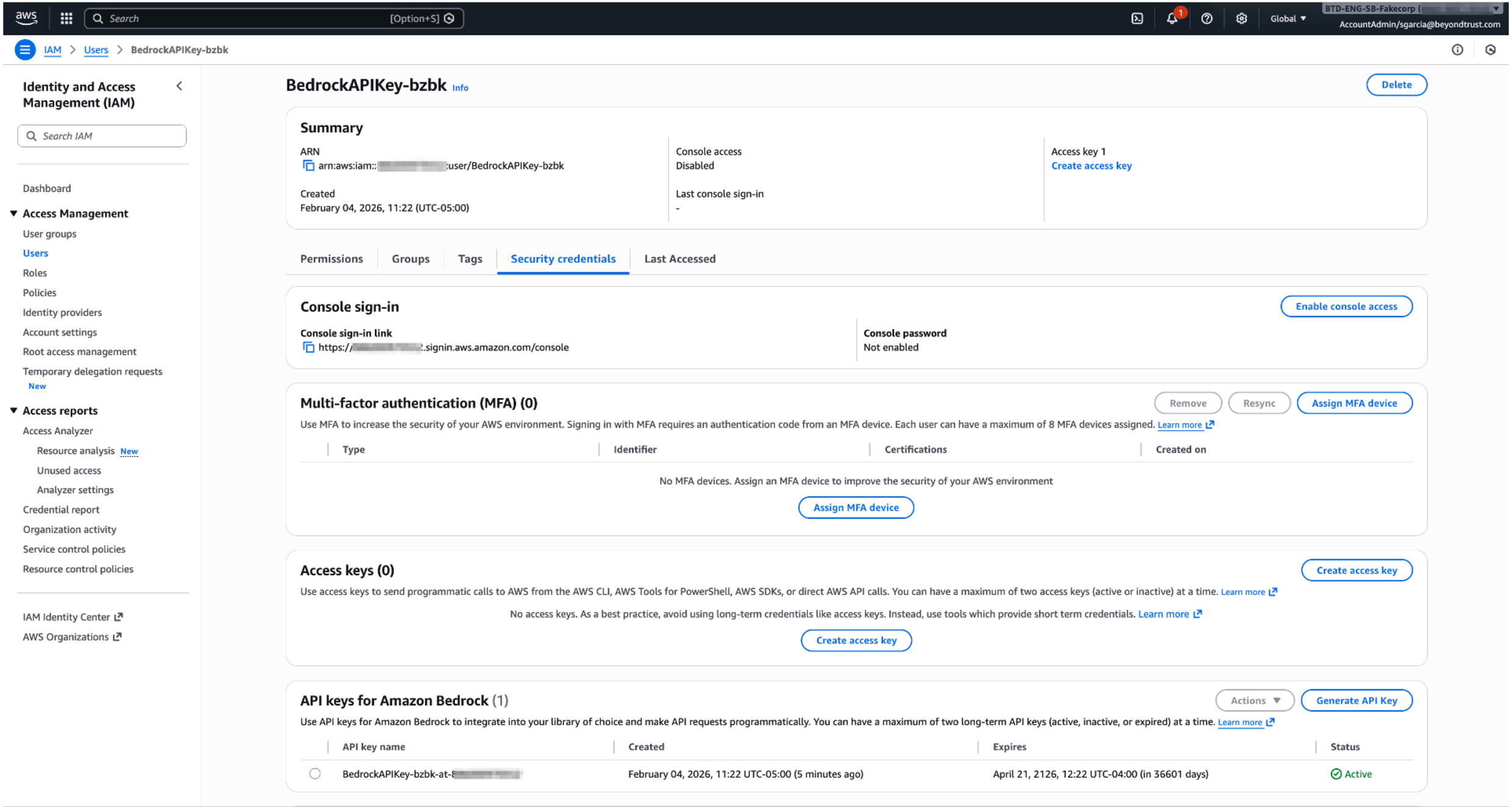
To set your API key as an environment variable so that it's automatically recognized when you make API requests, copy the shell example for your operating system and run it in a terminal. You can also specify API keys directly in an API request. Learn More.

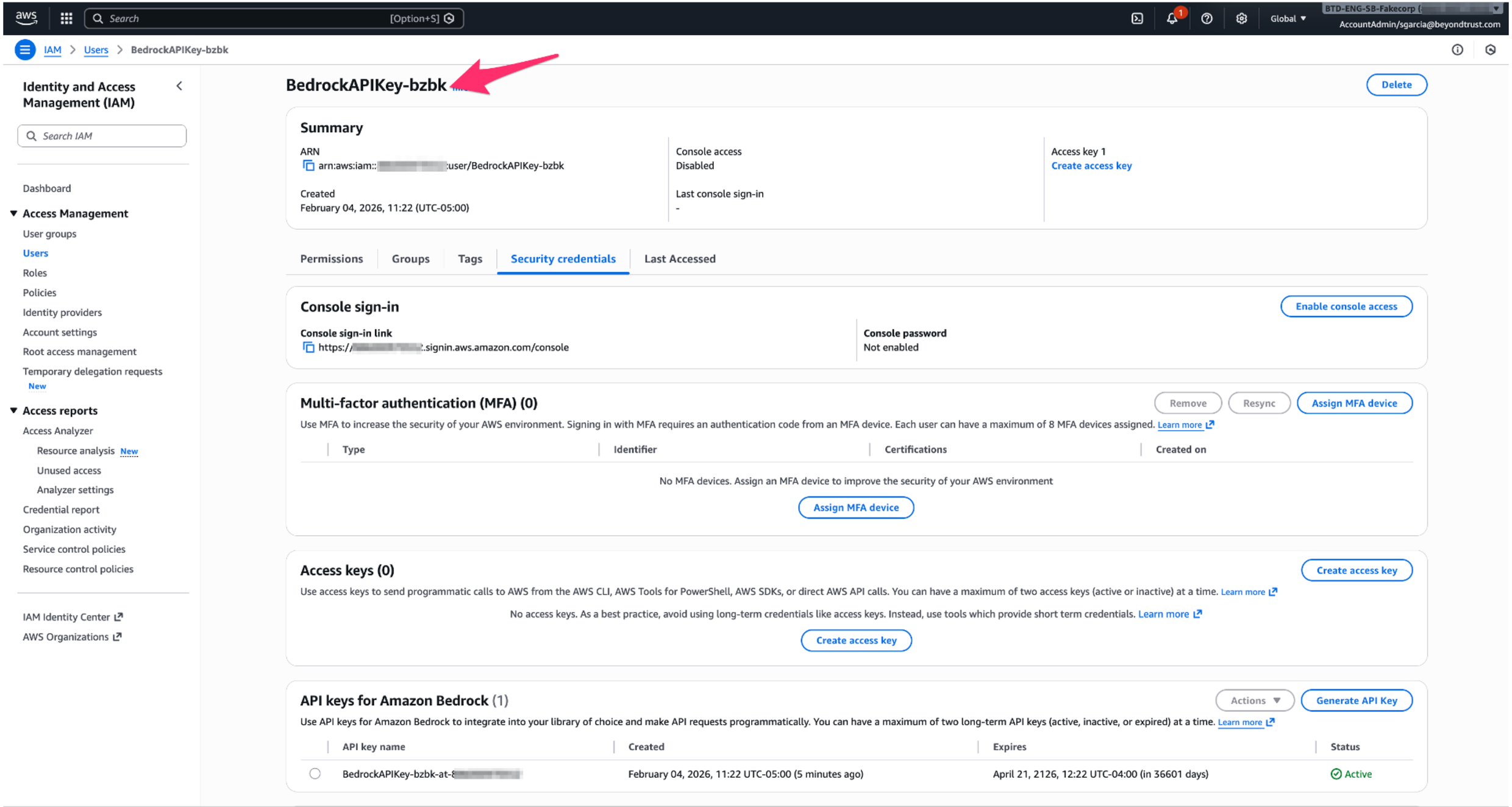
MacOS/Linux shell | Windows shell

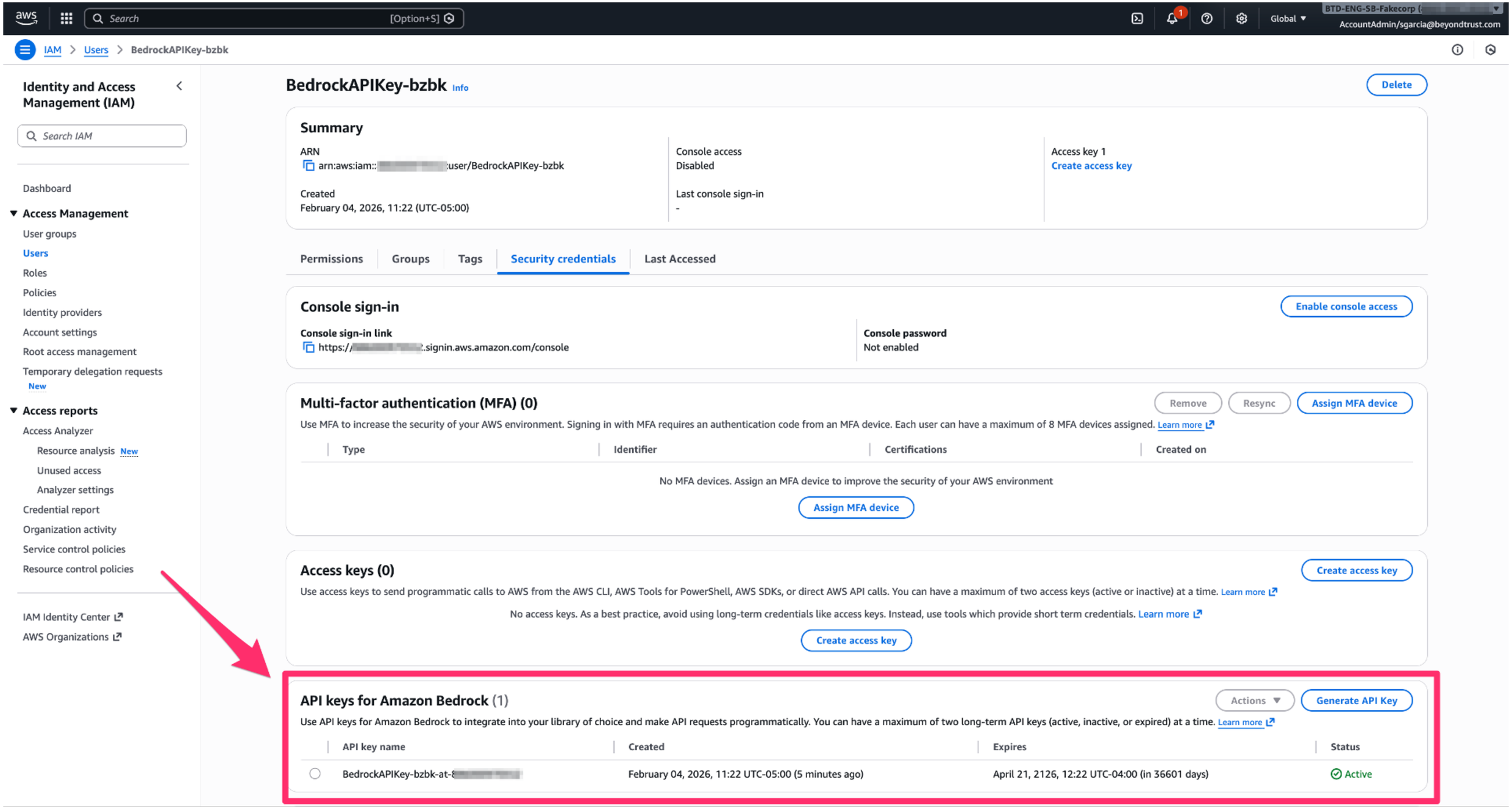
```
export AWS_BEARER_TOKEN_BEDROCK=ABSKQmVkcm9ja0FQSUtleS1[redacted]
```

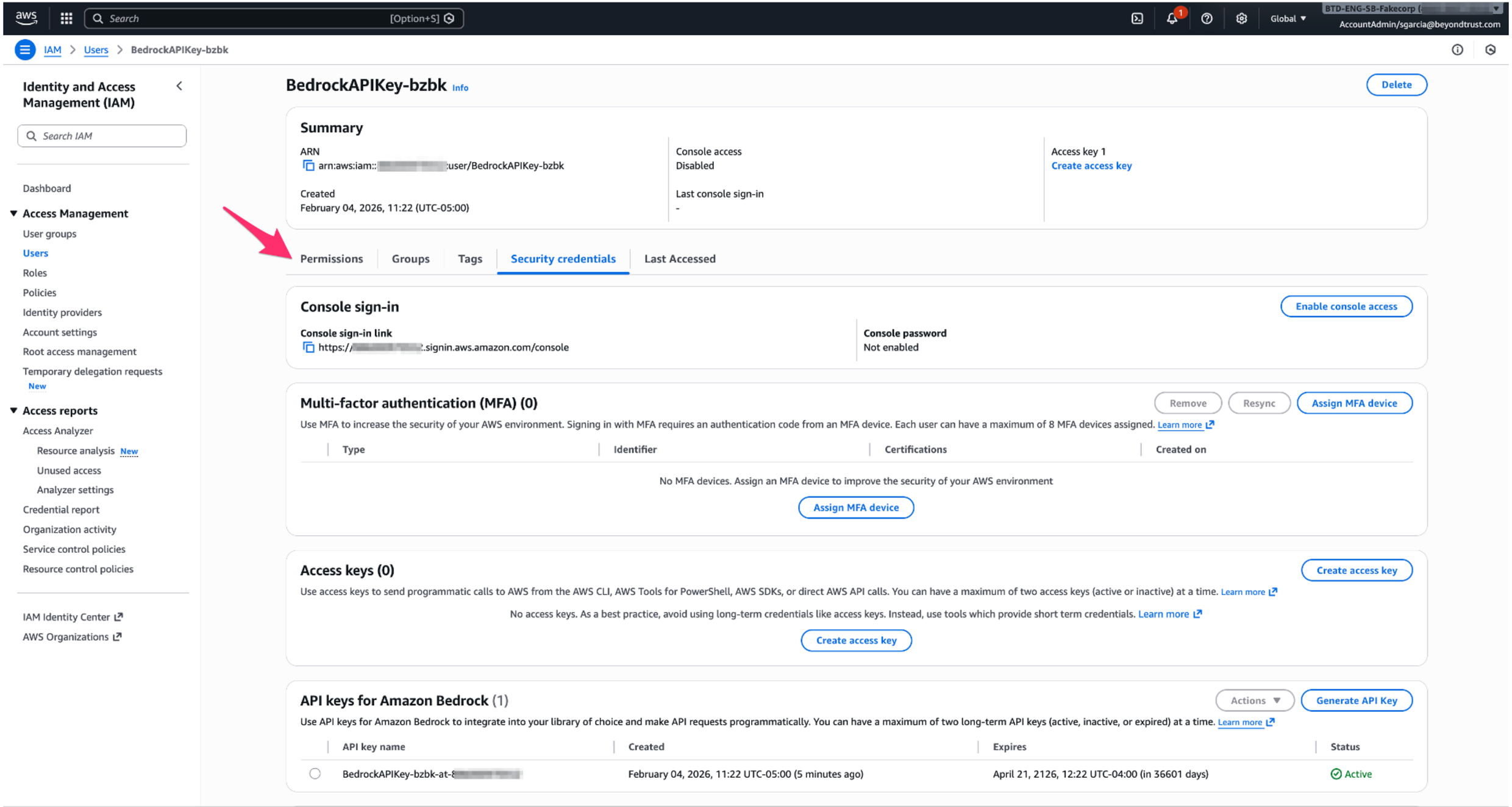
Copy API Key

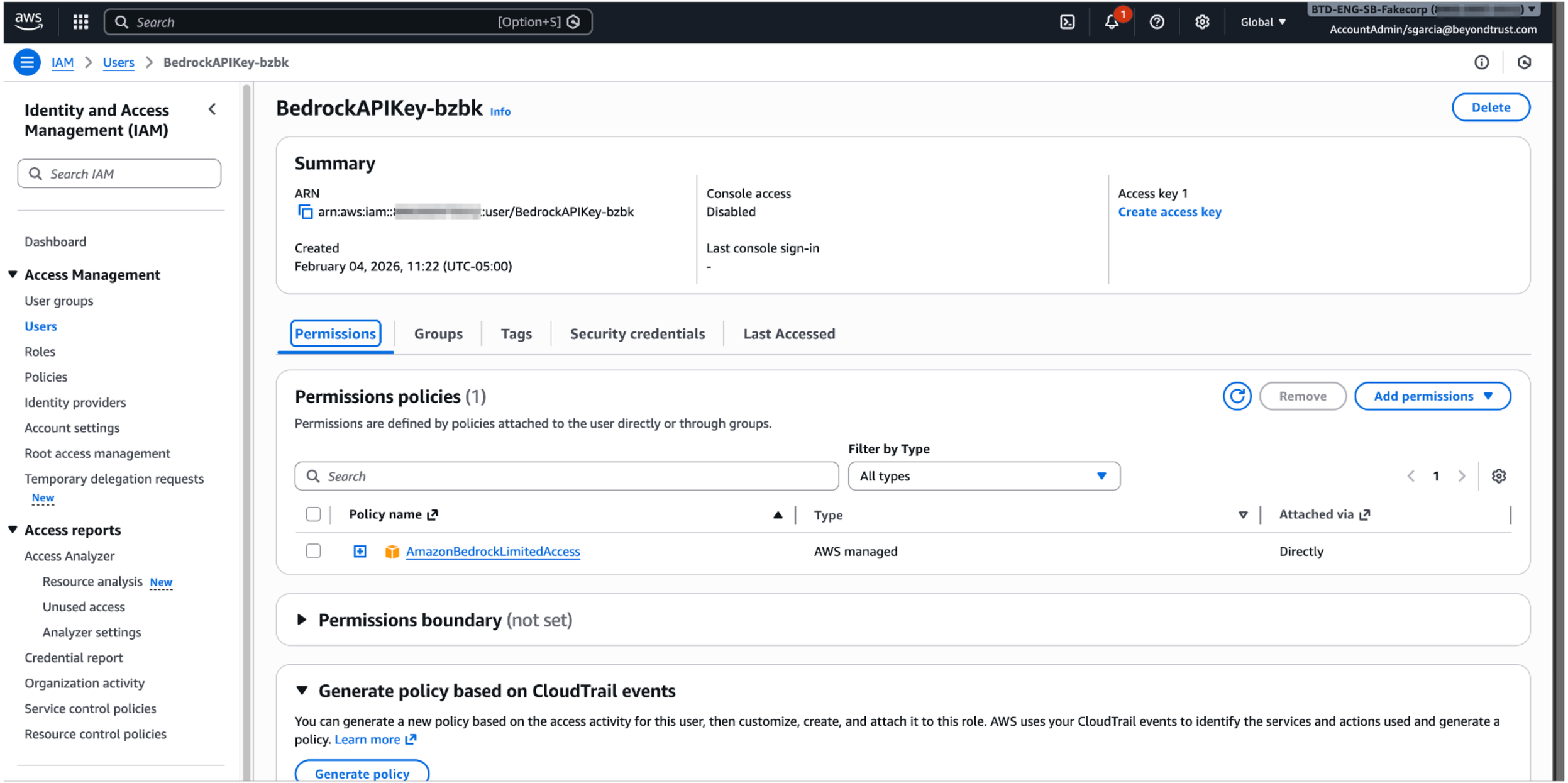
Download API Key | Close

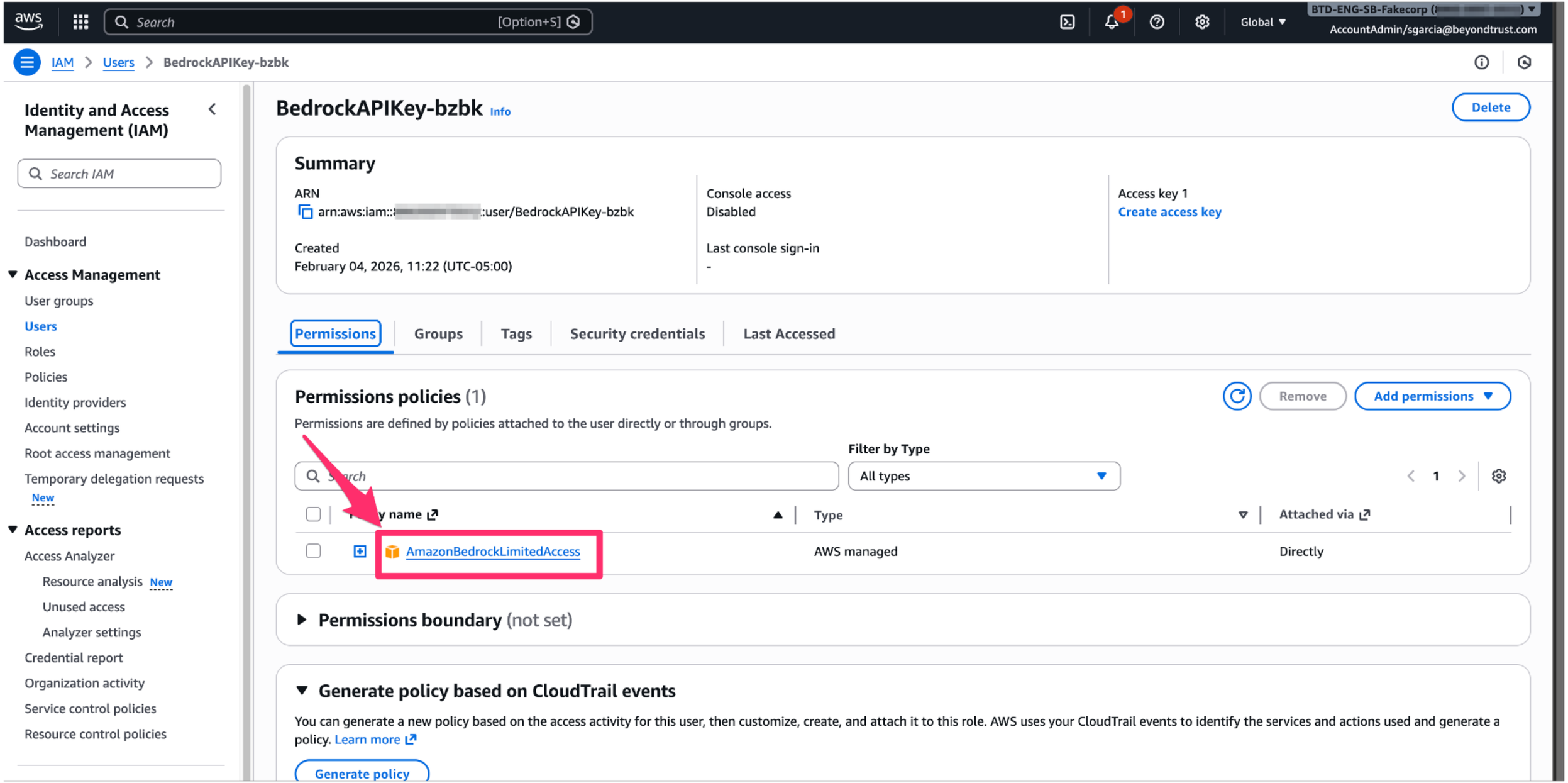

Search [Option+S]
Global
BTD-ENG-SB-Fakecorp (
AccountAdmin/sgarcia@beyondtrust.com
IAM > Users > BedrockAPIKey-bzbk
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
BedrockAPIKey-bzbk Info
Delete
Summary
ARN
arn:aws:iam::[redacted]:user/BedrockAPIKey-bzbk
Created
February 04, 2026, 11:22 (UTC-05:00)
Console access
Disabled
Last console sign-in
-
Access key 1
Create access key
Permissions
Groups
Tags
Security credentials
Last Accessed
Console sign-in
Enable console access
Console sign-in link
https://[redacted].signin.aws.amazon.com/console
Console password
Not enabled
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (0)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more
Create access key
API keys for Amazon Bedrock (1)
Actions
Generate API Key
Use API keys for Amazon Bedrock to integrate into your library of choice and make API requests programmatically. You can have a maximum of two long-term API keys (active, inactive, or expired) at a time. Learn more
API key name
Created
Expires
Status
BedrockAPIKey-bzbk-at-[redacted]
February 04, 2026, 11:22 UTC-05:00 (5 minutes ago)
April 21, 2126, 12:22 UTC-04:00 (in 36601 days)
Active

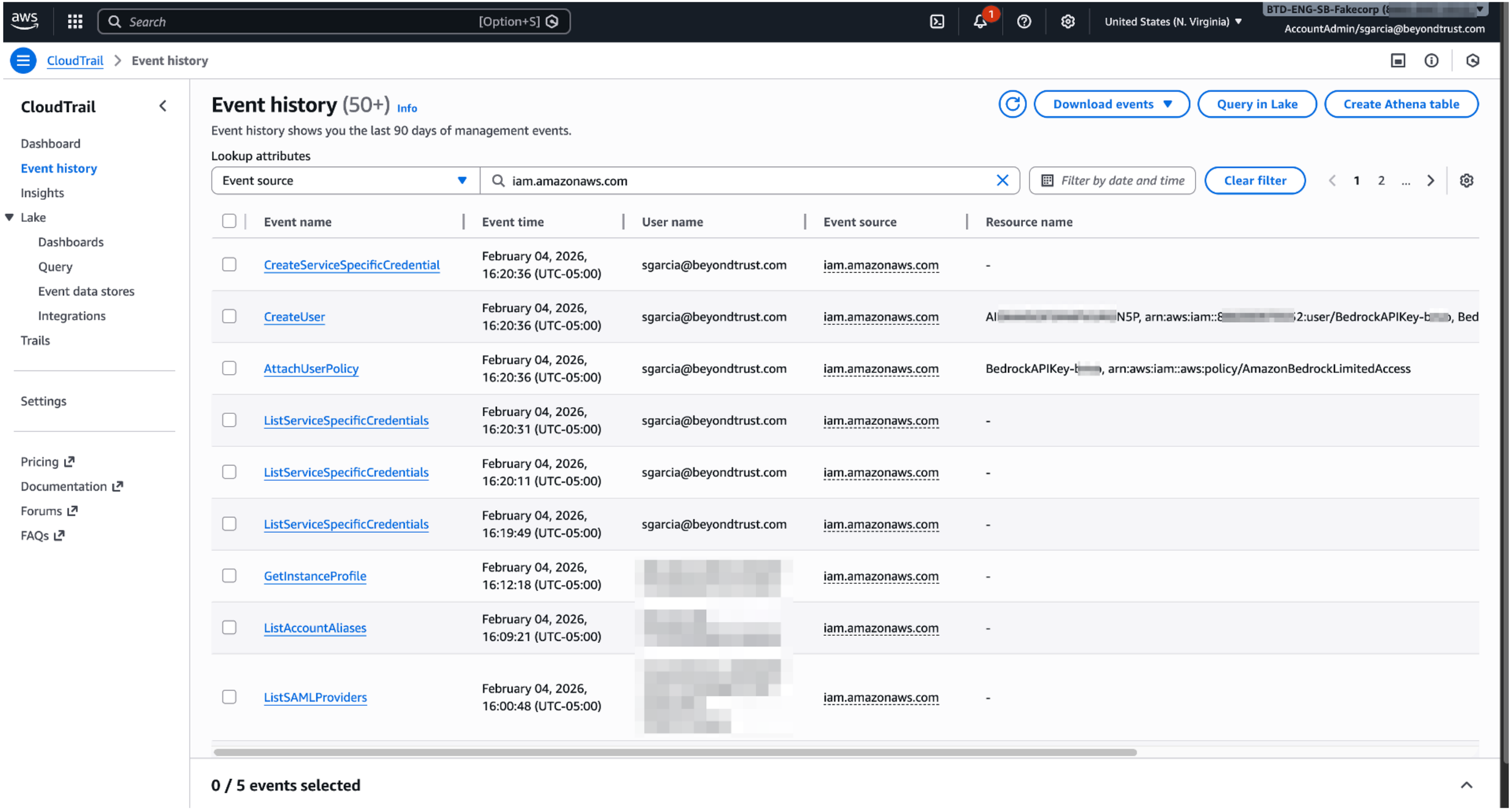

Search
[Option+S]
Global
BTD-ENG-SB-Fakecorp (
AccountAdmin/sgarcia@beyondtrust.com
IAM
Users
BedrockAPIKey-bzbk
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
BedrockAPIKey-bzbk
Delete
Summary
ARN
arn:aws:iam::
:user/BedrockAPIKey-bzbk
Created
February 04, 2026, 11:22 (UTC-05:00)
Console access
Disabled
Last console sign-in
-
Access key 1
Create access key
Permissions
Groups
Tags
Security credentials
Last Accessed
Console sign-in
Enable console access
Console sign-in link
https://
.signin.aws.amazon.com/console
Console password
Not enabled
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (0)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more
Create access key
API keys for Amazon Bedrock (1)
Actions
Generate API Key
Use API keys for Amazon Bedrock to integrate into your library of choice and make API requests programmatically. You can have a maximum of two long-term API keys (active, inactive, or expired) at a time. Learn more
API key name
Created
Expires
Status
BedrockAPIKey-bzbk-at-8
February 04, 2026, 11:22 UTC-05:00 (5 minutes ago)
April 21, 2126, 12:22 UTC-04:00 (in 36601 days)
Active

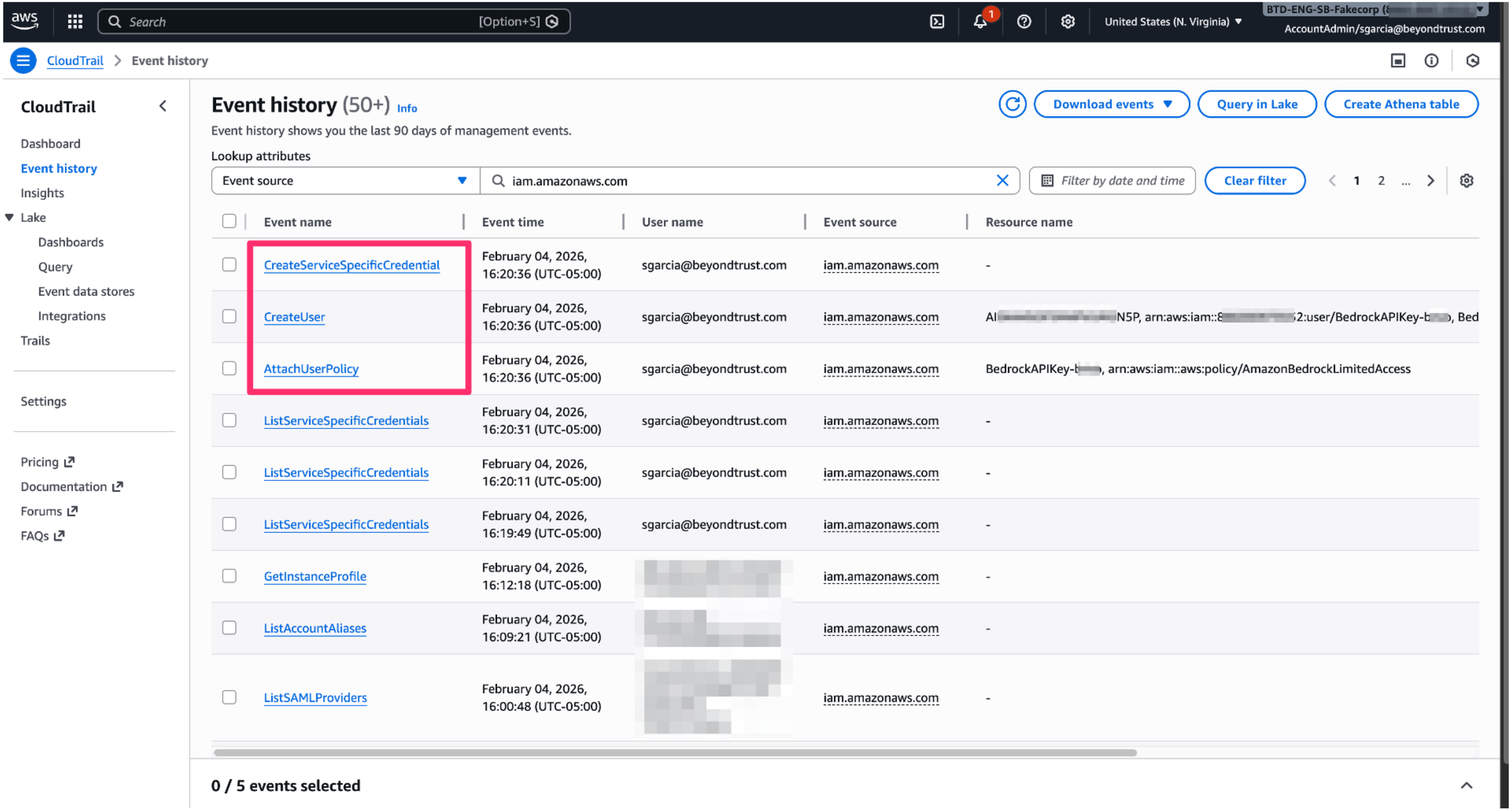

Search [Option+S]
Global
BTD-ENG-SB-Fakecorp (
AccountAdmin/sgarcia@beyondtrust.com
IAM > Users > BedrockAPIKey-bzbk
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
BedrockAPIKey-bzbk Info
Delete
Summary
ARN
arn:aws:iam::[redacted]:user/BedrockAPIKey-bzbk
Created
February 04, 2026, 11:22 (UTC-05:00)
Console access
Disabled
Last console sign-in
-
Access key 1
Create access key
Permissions
Groups
Tags
Security credentials
Last Accessed
Console sign-in
Enable console access
Console sign-in link
https://[redacted].signin.aws.amazon.com/console
Console password
Not enabled
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (0)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more
Create access key
API keys for Amazon Bedrock (1)
Actions
Generate API Key
Use API keys for Amazon Bedrock to integrate into your library of choice and make API requests programmatically. You can have a maximum of two long-term API keys (active, inactive, or expired) at a time. Learn more
API key name
Created
Expires
Status
BedrockAPIKey-bzbk-at-[redacted]
February 04, 2026, 11:22 UTC-05:00 (5 minutes ago)
April 21, 2126, 12:22 UTC-04:00 (in 36601 days)
Active

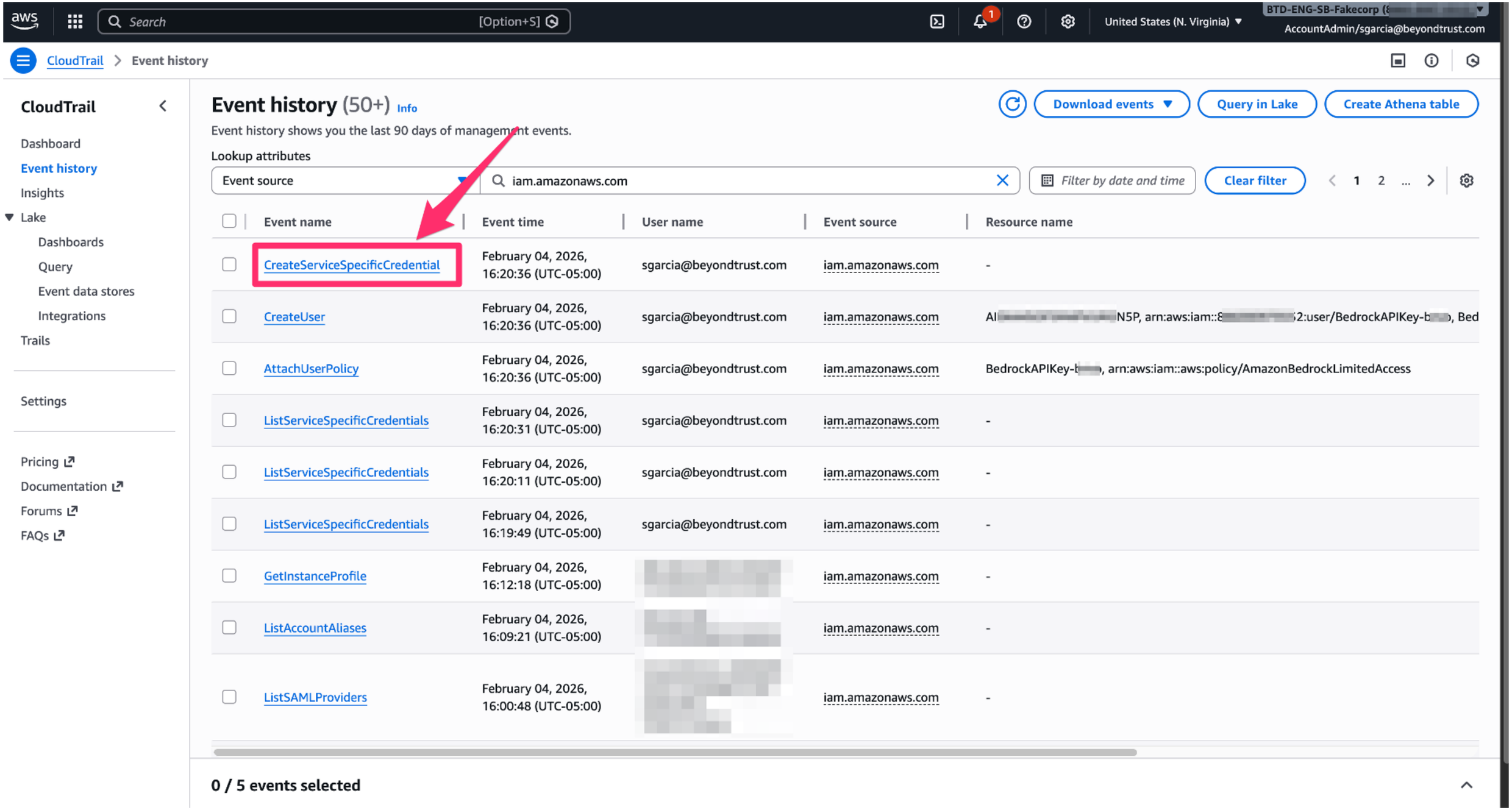

aws
Search
[Option+S]
Global
BTD-ENG-SB-Fakecorp (
AccountAdmin/sgarcia@beyondtrust.com
IAM > Users > BedrockAPIKey-bzbk
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
BedrockAPIKey-bzbk Info
Delete
Summary
ARN
arn:aws:iam::
:user/BedrockAPIKey-bzbk
Created
February 04, 2026, 11:22 (UTC-05:00)
Console access
Disabled
Last console sign-in
-
Access key 1
Create access key
Permissions
Groups
Tags
Security credentials
Last Accessed
Console sign-in
Enable console access
Console sign-in link
https://
.signin.aws.amazon.com/console
Console password
Not enabled
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (0)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more
Create access key
API keys for Amazon Bedrock (1)
Actions
Generate API Key
Use API keys for Amazon Bedrock to integrate into your library of choice and make API requests programmatically. You can have a maximum of two long-term API keys (active, inactive, or expired) at a time. Learn more
API key name
Created
Expires
Status
BedrockAPIKey-bzbk-at-8
February 04, 2026, 11:22 UTC-05:00 (5 minutes ago)
April 21, 2126, 12:22 UTC-04:00 (in 36601 days)
Active


Search
[Option+S]
Global
AccountAdmin/sgarcia@beyondtrust.com
IAM > Users > BedrockAPIKey-bzbk
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
BedrockAPIKey-bzbk Info
Delete
Summary
ARN
arn:aws:iam::[redacted]:user/BedrockAPIKey-bzbk
Created
February 04, 2026, 11:22 (UTC-05:00)
Console access
Disabled
Last console sign-in
-
Access key 1
Create access key
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached via
AmazonBedrockLimitedAccess
AWS managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy


aws
Search
[Option+S]
Global
BTD-ENG-SB-Fakecorp
AccountAdmin/sgarcia@beyondtrust.com
IAM > Users > BedrockAPIKey-bzbk
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
BedrockAPIKey-bzbk Info
Delete
Summary
ARN
arn:aws:iam::[redacted]:user/BedrockAPIKey-bzbk
Console access
Disabled
Access key 1
Create access key
Created
February 04, 2026, 11:22 (UTC-05:00)
Last console sign-in
-
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
All types
Type
Attached via
AmazonBedrockLimitedAccess
AWS managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy


aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
CloudTrail
Event history
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboards
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
Event history (50+) Info
Event history shows you the last 90 days of management events.
Download events
Query in Lake
Create Athena table
Lookup attributes
Event source
iam.amazonaws.com
Filter by date and time
Clear filter
1 2 ...
Event name
Event time
User name
Event source
Resource name
CreateServiceSpecificCredential
February 04, 2026, 16:20:36 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
-
CreateUser
February 04, 2026, 16:20:36 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
AI N5P, arn:aws:iam::8 2:user/BedrockAPIKey-b , Bed
AttachUserPolicy
February 04, 2026, 16:20:36 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
BedrockAPIKey-b , arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess
ListServiceSpecificCredentials
February 04, 2026, 16:20:31 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
-
ListServiceSpecificCredentials
February 04, 2026, 16:20:11 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
-
ListServiceSpecificCredentials
February 04, 2026, 16:19:49 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
-
GetInstanceProfile
February 04, 2026, 16:12:18 (UTC-05:00)
iam.amazonaws.com
-
ListAccountAliases
February 04, 2026, 16:09:21 (UTC-05:00)
iam.amazonaws.com
-
ListSAMLProviders
February 04, 2026, 16:00:48 (UTC-05:00)
iam.amazonaws.com
-
0 / 5 events selected

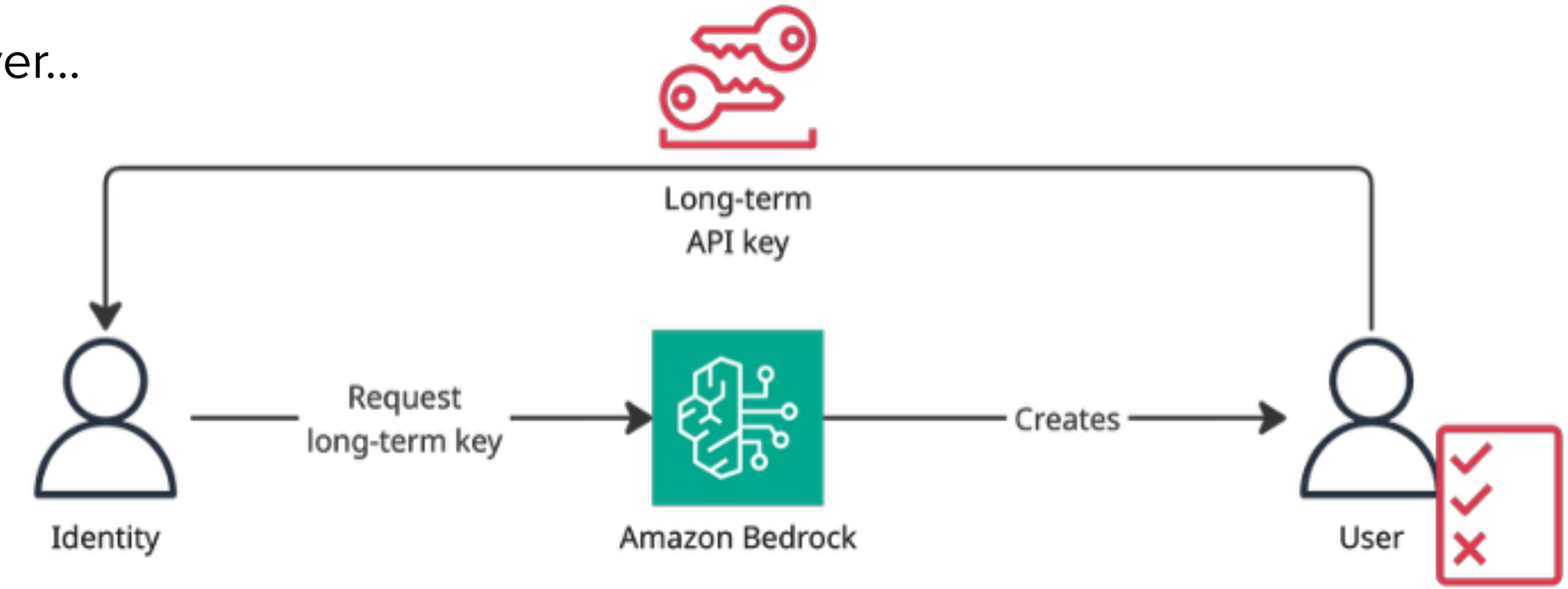

aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
CloudTrail > Event history
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboards
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
Event history (50+) Info
Event history shows you the last 90 days of management events.
Download events
Query in Lake
Create Athena table
Lookup attributes
Event source
iam.amazonaws.com
Filter by date and time
Clear filter
1 2 ...
Event name | Event time | User name | Event source | Resource name
CreateServiceSpecificCredential | February 04, 2026, 16:20:36 (UTC-05:00) | sgarcia@beyondtrust.com | iam.amazonaws.com | -
CreateUser | February 04, 2026, 16:20:36 (UTC-05:00) | sgarcia@beyondtrust.com | iam.amazonaws.com | AI[redacted]N5P, arn:aws:iam::8[redacted]2:user/BedrockAPIKey-b[redacted], Bed
AttachUserPolicy | February 04, 2026, 16:20:36 (UTC-05:00) | sgarcia@beyondtrust.com | iam.amazonaws.com | BedrockAPIKey-b[redacted], arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess
ListServiceSpecificCredentials | February 04, 2026, 16:20:31 (UTC-05:00) | sgarcia@beyondtrust.com | iam.amazonaws.com | -
ListServiceSpecificCredentials | February 04, 2026, 16:20:11 (UTC-05:00) | sgarcia@beyondtrust.com | iam.amazonaws.com | -
ListServiceSpecificCredentials | February 04, 2026, 16:19:49 (UTC-05:00) | sgarcia@beyondtrust.com | iam.amazonaws.com | -
GetInstanceProfile | February 04, 2026, 16:12:18 (UTC-05:00) | [redacted] | iam.amazonaws.com | -
ListAccountAliases | February 04, 2026, 16:09:21 (UTC-05:00) | [redacted] | iam.amazonaws.com | -
ListSAMLProviders | February 04, 2026, 16:00:48 (UTC-05:00) | [redacted] | iam.amazonaws.com | -
0 / 5 events selected


aws
Search
[Option+S]
United States (N. Virginia)
AccountAdmin/sgarcia@beyondtrust.com
CloudTrail
Event history
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboards
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
Event history (50+) Info
Event history shows you the last 90 days of management events.
Download events
Query in Lake
Create Athena table
Lookup attributes
Event source
iam.amazonaws.com
Filter by date and time
Clear filter
1 2 ...
Event name
Event time
User name
Event source
Resource name
CreateServiceSpecificCredential
February 04, 2026, 16:20:36 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
-
CreateUser
February 04, 2026, 16:20:36 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
AI[redacted]N5P, arn:aws:iam::8[redacted]2:user/BedrockAPIKey-b[redacted], Bed
AttachUserPolicy
February 04, 2026, 16:20:36 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
BedrockAPIKey-b[redacted], arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess
ListServiceSpecificCredentials
February 04, 2026, 16:20:31 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
-
ListServiceSpecificCredentials
February 04, 2026, 16:20:11 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
-
ListServiceSpecificCredentials
February 04, 2026, 16:19:49 (UTC-05:00)
sgarcia@beyondtrust.com
iam.amazonaws.com
-
GetInstanceProfile
February 04, 2026, 16:12:18 (UTC-05:00)
iam.amazonaws.com
-
ListAccountAliases
February 04, 2026, 16:09:21 (UTC-05:00)
iam.amazonaws.com
-
ListSAMLProviders
February 04, 2026, 16:00:48 (UTC-05:00)
iam.amazonaws.com
-
0 / 5 events selected

```
"eventTime": "2026-02-04T16:22:32Z",
"eventSource": "iam.amazonaws.com",
"eventName": "CreateServiceSpecificCredential",
"awsRegion": "us-east-1",
"sourceIPAddress": "104.28.237.80",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36",
"requestParameters": {
    "userName": "BedrockAPIKey-bzbk",
    "serviceName": "bedrock.amazonaws.com",
    "credentialAgeDays": 36600
},
"responseElements": {
    "serviceSpecificCredential": {
        "createDate": "Feb 4, 2026, 4:22:32 PM",
        "expirationDate": "Apr 21, 2126, 4:22:32 PM",
        "serviceName": "bedrock.amazonaws.com",
        "serviceCredentialAlias": "BedrockAPIKey-bzbk-at-[redacted]",
        "serviceSpecificCredentialId": "ACCA[redacted]",
        "userName": "BedrockAPIKey-bzbk",
        "status": "Active"
    }
},
```

LONG-TERM KEYS

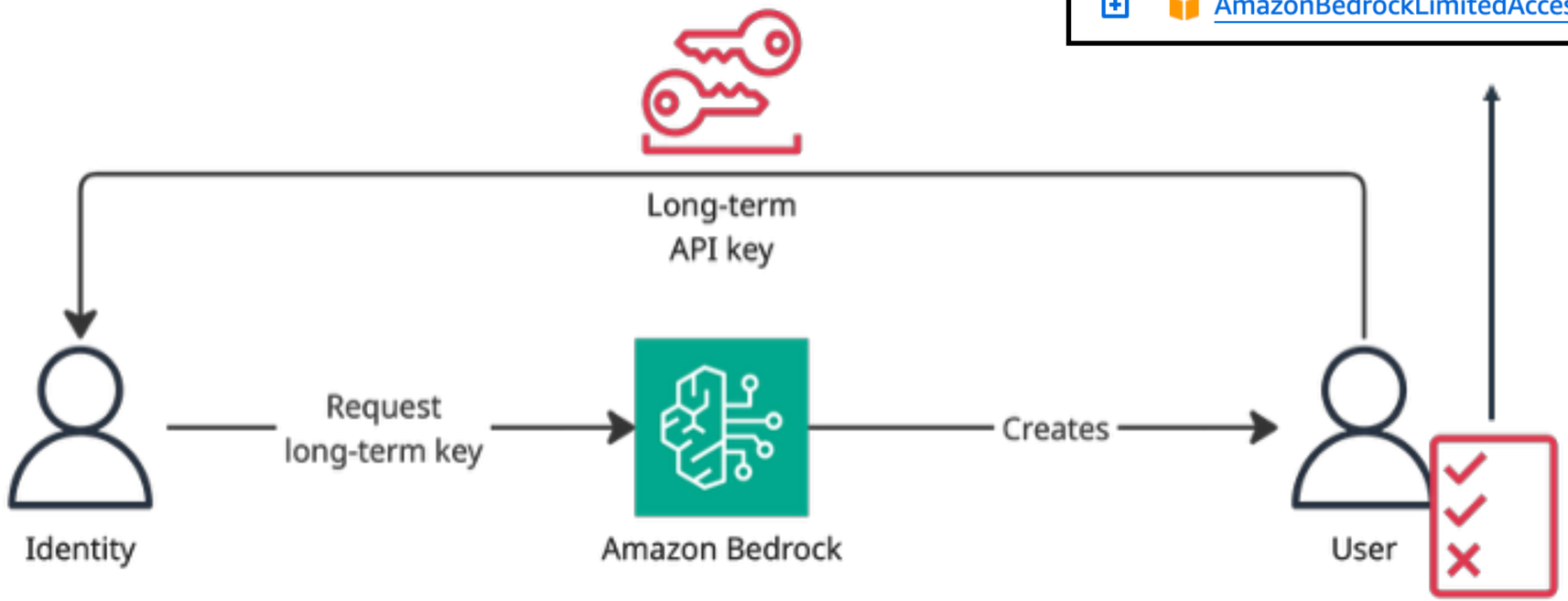
- Generated in Console / CLI / SDK
- **Base64 encoded string → ABSK**QmVkcm9ja0FQSUtleS....
- AWS creates dedicated IAM user **BedrockAPIKey-XXX**
- **Cloudtrail events:** `CreateUser + AttachUserPolicy + CreateServiceSpecificCredential`
- **Expiration:** 1 day to never...

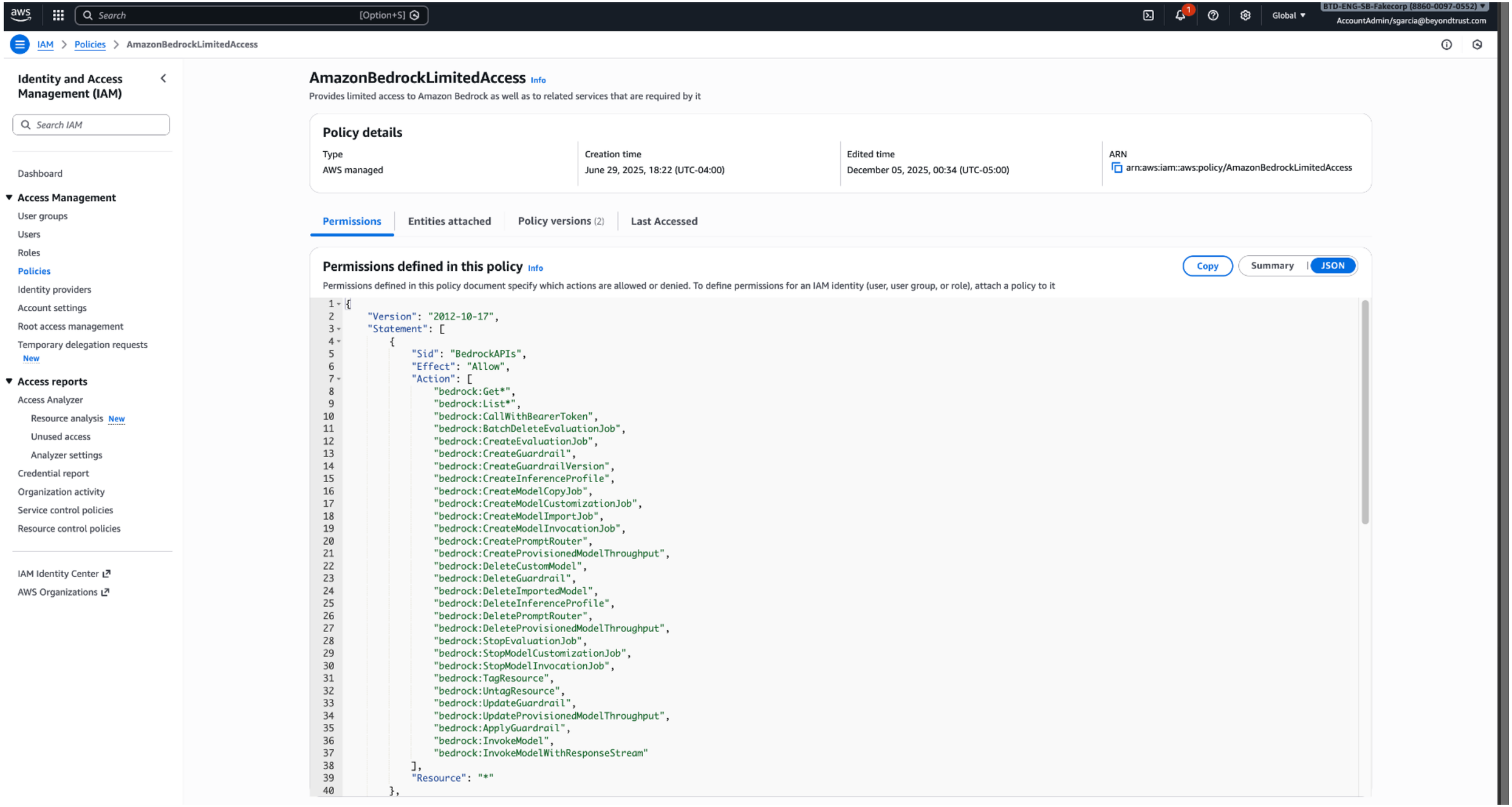


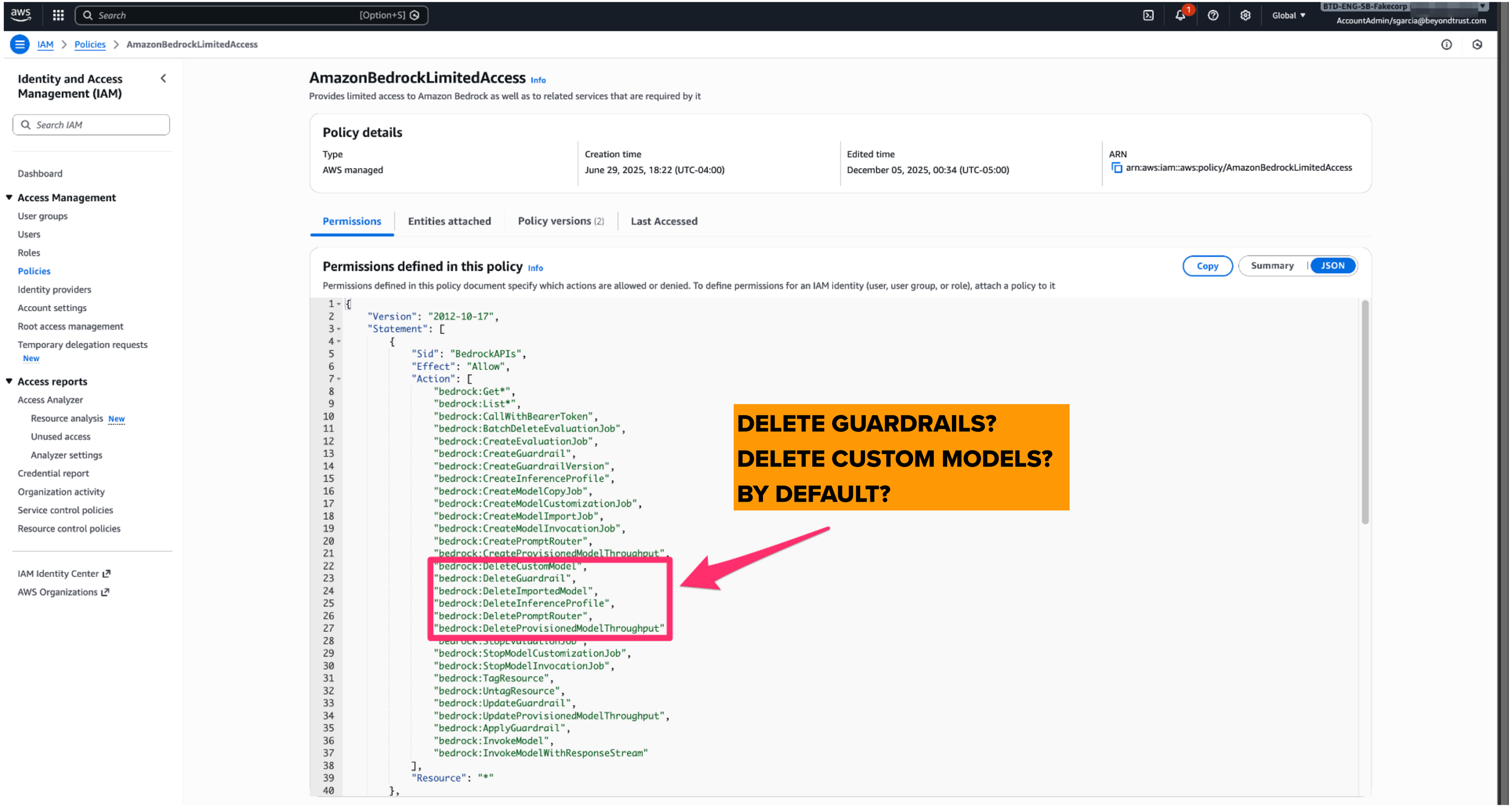
BUT DON'T WORRY...

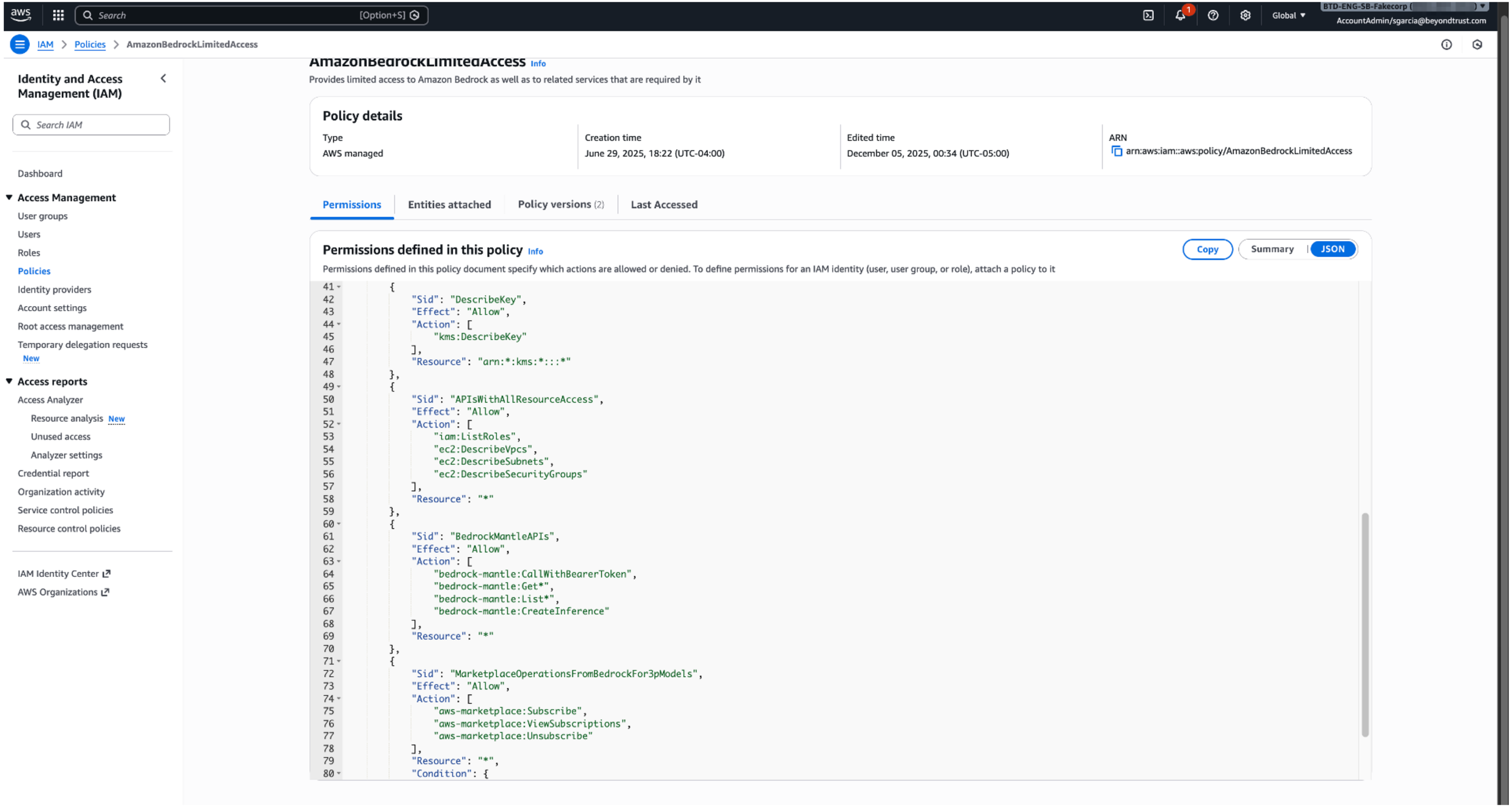
- AWS attaches a "limited" policy by default to the IAM user
- Sounds safe, right?
- Let's check what's actually in there...

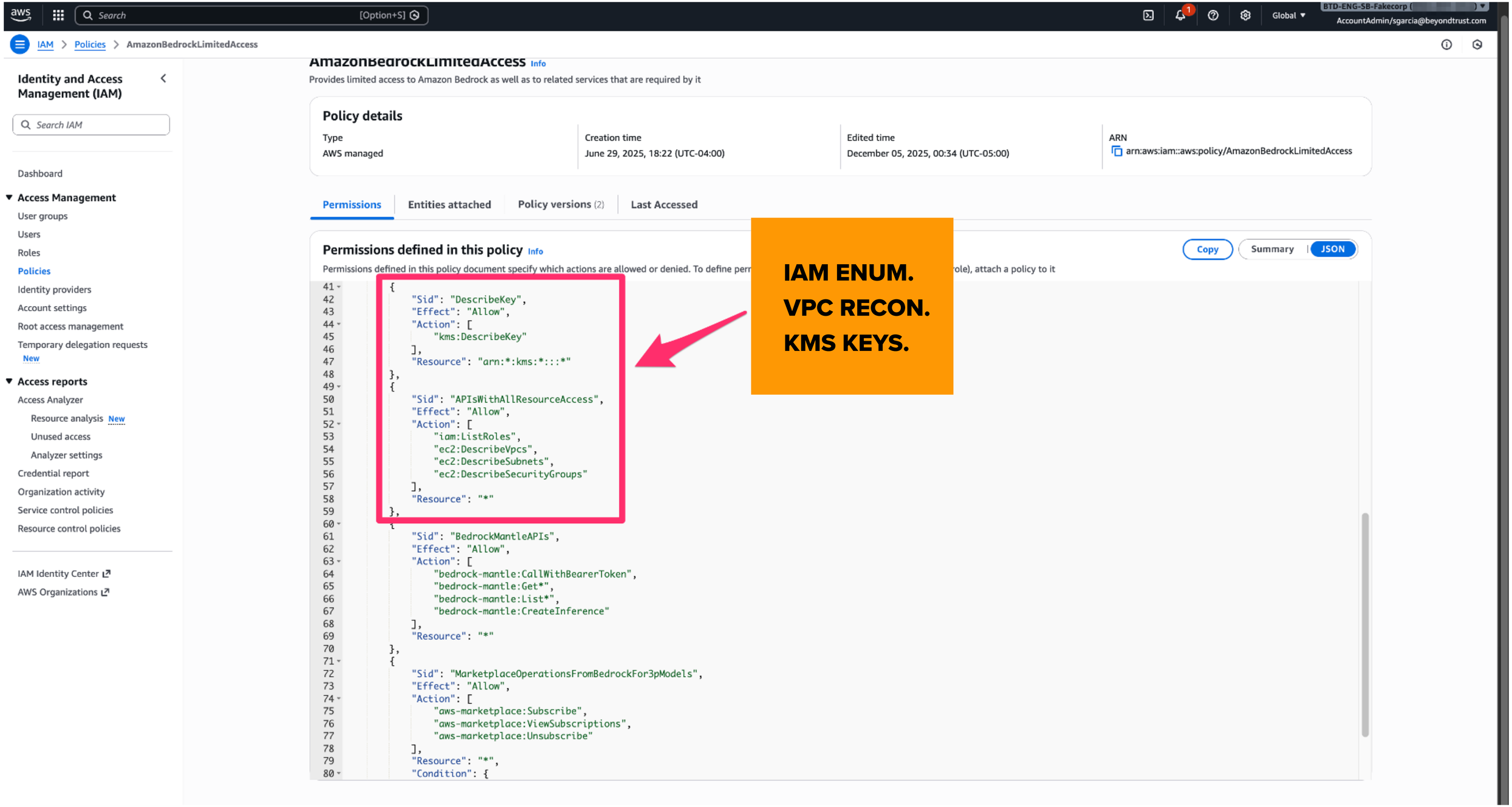


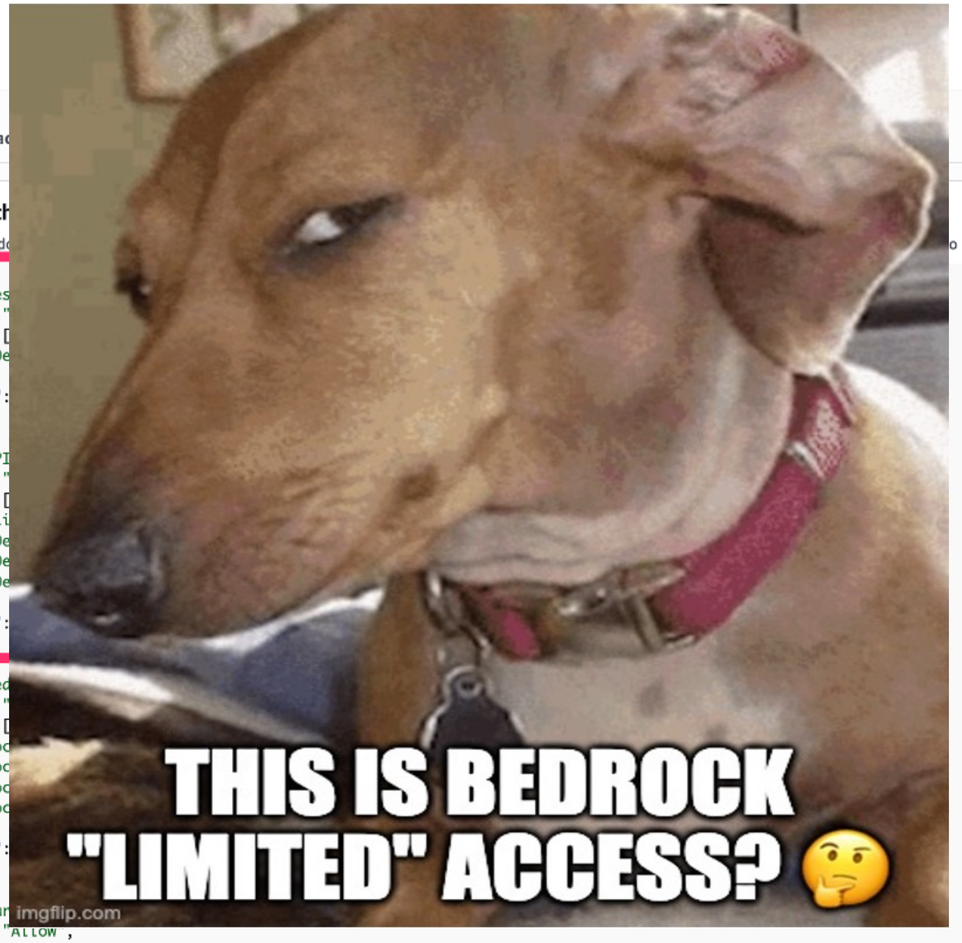



aws
Search
[Option+S]
Global
BTD-ENG-SB-Fakecorp (8860-0097-0552)
AccountAdmin/sgarcia@beyondtrust.com
IAM > Policies > AmazonBedrockLimitedAccess
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
AmazonBedrockLimitedAccess Info
Provides limited access to Amazon Bedrock as well as to related services that are required by it
Policy details
Type
AWS managed
Creation time
June 29, 2025, 18:22 (UTC-04:00)
Edited time
December 05, 2025, 00:34 (UTC-05:00)
ARN
arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess
Permissions
Entities attached
Policy versions (2)
Last Accessed
Permissions defined in this policy Info
Copy
Summary
JSON
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "BedrockAPIs",
"Effect": "Allow",
"Action": [
"bedrock:Get*",
"bedrock:List*",
"bedrock:CallWithBearerToken",
"bedrock:BatchDeleteEvaluationJob",
"bedrock:CreateEvaluationJob",
"bedrock:CreateGuardrail",
"bedrock:CreateGuardrailVersion",
"bedrock:CreateInferenceProfile",
"bedrock:CreateModelCopyJob",
"bedrock:CreateModelCustomizationJob",
"bedrock:CreateModelImportJob",
"bedrock:CreateModelInvocationJob",
"bedrock:CreatePromptRouter",
"bedrock:CreateProvisionedModelThroughput",
"bedrock:DeleteCustomModel",
"bedrock:DeleteGuardrail",
"bedrock:DeleteImportedModel",
"bedrock:DeleteInferenceProfile",
"bedrock:DeletePromptRouter",
"bedrock:DeleteProvisionedModelThroughput",
"bedrock:StopEvaluationJob",
"bedrock:StopModelCustomizationJob",
"bedrock:StopModelInvocationJob",
"bedrock:TagResource",
"bedrock:UntagResource",
"bedrock:UpdateGuardrail",
"bedrock:UpdateProvisionedModelThroughput",
"bedrock:ApplyGuardrail",
"bedrock:InvokeModel",
"bedrock:InvokeModelWithResponseStream"
],
"Resource": "*"
},

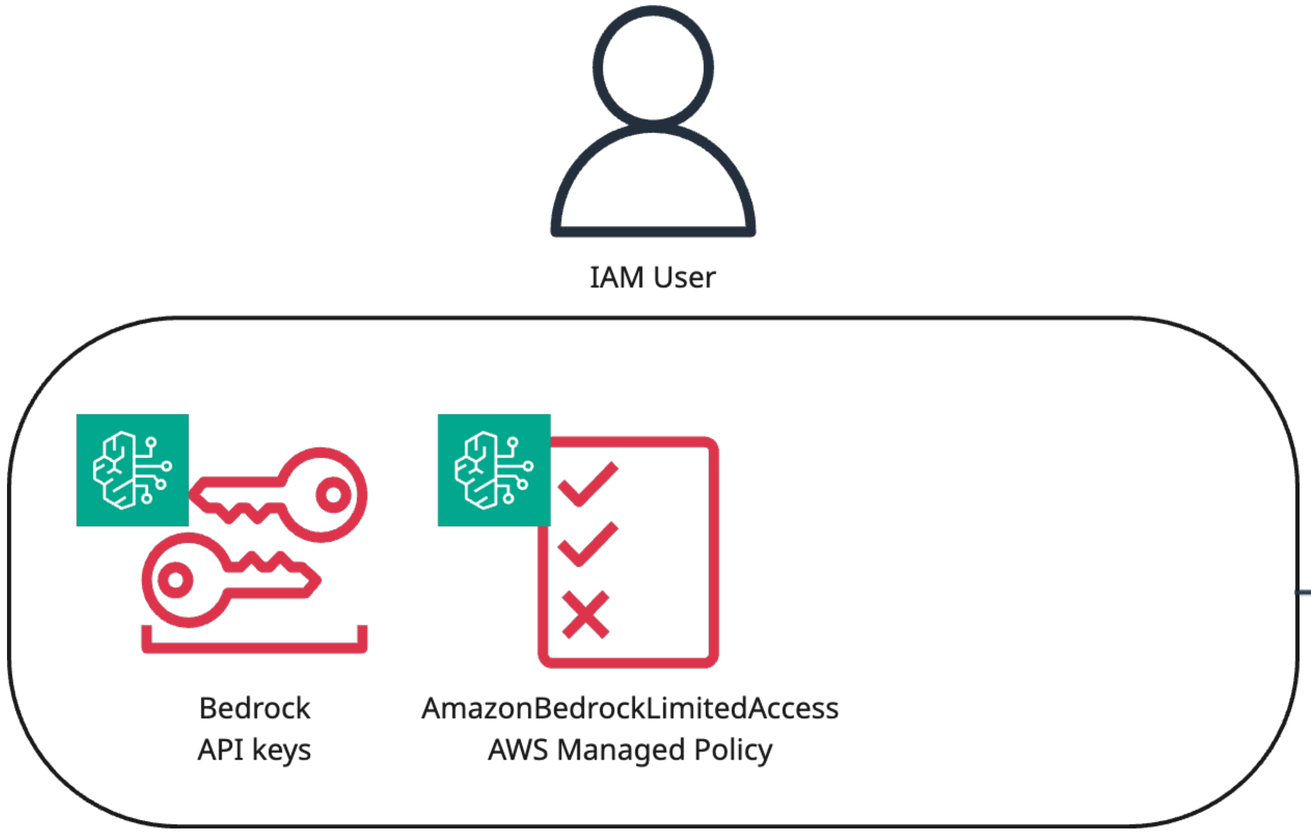

aws
Search
[Option+S]
Global
BTD-ENG-SB-Fakecorp
AccountAdmin/sgarcia@beyondtrust.com
IAM > Policies > AmazonBedrockLimitedAccess
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
AmazonBedrockLimitedAccess Info
Provides limited access to Amazon Bedrock as well as to related services that are required by it
Policy details
Type
AWS managed
Creation time
June 29, 2025, 18:22 (UTC-04:00)
Edited time
December 05, 2025, 00:34 (UTC-05:00)
ARN
arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess
Permissions
Entities attached
Policy versions (2)
Last Accessed
Permissions defined in this policy Info
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Copy
Summary
JSON
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "BedrockAPIs",
"Effect": "Allow",
"Action": [
"bedrock:Get*",
"bedrock:List*",
"bedrock:CallWithBearerToken",
"bedrock:BatchDeleteEvaluationJob",
"bedrock:CreateEvaluationJob",
"bedrock:CreateGuardrail",
"bedrock:CreateGuardrailVersion",
"bedrock:CreateInferenceProfile",
"bedrock:CreateModelCopyJob",
"bedrock:CreateModelCustomizationJob",
"bedrock:CreateModelImportJob",
"bedrock:CreateModelInvocationJob",
"bedrock:CreatePromptRouter",
"bedrock:CreateProvisionedModelThroughput",
"bedrock:DeleteCustomModel",
"bedrock:DeleteGuardrail",
"bedrock:DeleteImportedModel",
"bedrock:DeleteInferenceProfile",
"bedrock:DeletePromptRouter",
"bedrock:DeleteProvisionedModelThroughput"
"bedrock:StopModelCustomizationJob",
"bedrock:StopModelInvocationJob",
"bedrock:TagResource",
"bedrock:UntagResource",
"bedrock:UpdateGuardrail",
"bedrock:UpdateProvisionedModelThroughput",
"bedrock:ApplyGuardrail",
"bedrock:InvokeModel",
"bedrock:InvokeModelWithResponseStream"
],
"Resource": "*"
},
DELETE GUARDRAILS?
DELETE CUSTOM MODELS?
BY DEFAULT?


aws
Search
[Option+S]
Global
BTD-ENG-SB-Fakecorp
AccountAdmin/sgarcia@beyondtrust.com
IAM > Policies > AmazonBedrockLimitedAccess
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
AmazonBedrockLimitedAccess Info
Provides limited access to Amazon Bedrock as well as to related services that are required by it
Policy details
Type
AWS managed
Creation time
June 29, 2025, 18:22 (UTC-04:00)
Edited time
December 05, 2025, 00:34 (UTC-05:00)
ARN
arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess
Permissions
Entities attached
Policy versions (2)
Last Accessed
Permissions defined in this policy Info
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Copy
Summary
JSON
{
"Sid": "DescribeKey",
"Effect": "Allow",
"Action": [
"kms:DescribeKey"
],
"Resource": "arn:*:kms:*:::*"
},
{
"Sid": "APIsWithAllResourceAccess",
"Effect": "Allow",
"Action": [
"iam:ListRoles",
"ec2:DescribeVpcs",
"ec2:DescribeSubnets",
"ec2:DescribeSecurityGroups"
],
"Resource": "*"
},
{
"Sid": "BedrockMantleAPIs",
"Effect": "Allow",
"Action": [
"bedrock-mantle:CallWithBearerToken",
"bedrock-mantle:Get*",
"bedrock-mantle:List*",
"bedrock-mantle:CreateInference"
],
"Resource": "*"
},
{
"Sid": "MarketplaceOperationsFromBedrockFor3pModels",
"Effect": "Allow",
"Action": [
"aws-marketplace:Subscribe",
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Unsubscribe"
],
"Resource": "*",
"Condition": {


aws
Search
[Option+S]
Global
BTD-ENG-SB-Fakecorp
AccountAdmin/sgarcia@beyondtrust.com
IAM > Policies > AmazonBedrockLimitedAccess
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
AmazonBedrockLimitedAccess Info
Provides limited access to Amazon Bedrock as well as to related services that are required by it
Policy details
Type
AWS managed
Creation time
June 29, 2025, 18:22 (UTC-04:00)
Edited time
December 05, 2025, 00:34 (UTC-05:00)
ARN
arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess
Permissions
Entities attached
Policy versions (2)
Last Accessed
Permissions defined in this policy Info
Copy
Summary
JSON
IAM ENUM.
VPC RECON.
KMS KEYS.
{
"Sid": "DescribeKey",
"Effect": "Allow",
"Action": [
"kms:DescribeKey"
],
"Resource": "arn:*:kms:*:::*"
},
{
"Sid": "APIsWithAllResourceAccess",
"Effect": "Allow",
"Action": [
"iam:ListRoles",
"ec2:DescribeVpcs",
"ec2:DescribeSubnets",
"ec2:DescribeSecurityGroups"
],
"Resource": "*"
},
{
"Sid": "BedrockMantleAPIs",
"Effect": "Allow",
"Action": [
"bedrock-mantle:CallWithBearerToken",
"bedrock-mantle:Get*",
"bedrock-mantle:List*",
"bedrock-mantle:CreateInference"
],
"Resource": "*"
},
{
"Sid": "MarketplaceOperationsFromBedrockFor3pModels",
"Effect": "Allow",
"Action": [
"aws-marketplace:Subscribe",
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Unsubscribe"
],
"Resource": "*",
"Condition": {

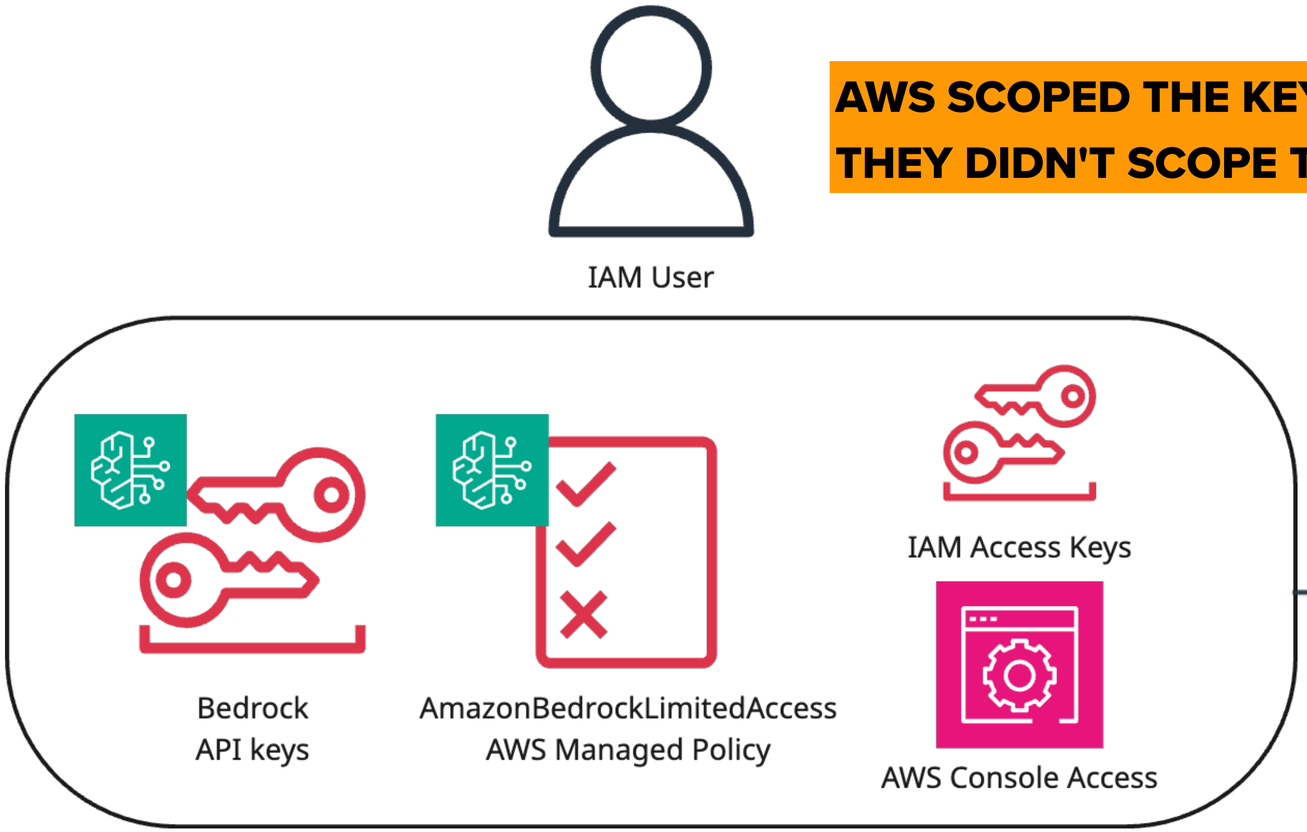

THIS IS BEDROCK
"LIMITED" ACCESS?
imgflip.com

THE SCOPING CATCH




```
"Sid": "BedrockAPIs",
"Effect": "Allow",
"Action": [
    "bedrock:Get*",
    "bedrock:List*",
    "bedrock:CallWithBearerToken",
    "bedrock:BatchDeleteEvaluationJob",
    "bedrock:CreateEvaluationJob",
    "bedrock:CreateGuardrail",
    "bedrock:CreateGuardrailVersion",
    "bedrock:CreateInferenceProfile",
    "bedrock:CreateModelCopyJob",
    "bedrock:CreateModelCustomizationJob",
    "bedrock:CreateModelImportJob",
    "bedrock:CreateModelInvocationJob",
    "bedrock:CreatePromptRouter",
    "bedrock:CreateProvisionedModelThroughput",
    "bedrock:DeleteCustomModel",
    "bedrock:DeleteGuardrail",
    "bedrock:DeleteImportedModel",
    "bedrock:DeleteInferenceProfile",
    "bedrock:DeletePromptRouter",
    "bedrock:DeleteProvisionedModelThroughput",
    "bedrock:StopEvaluationJob",
    "bedrock:StopModelCustomizationJob",
    "bedrock:StopModelInvocationJob",
    "bedrock:TagResource",
    "bedrock:UntagResource",
    "bedrock:UpdateGuardrail",
    "bedrock:UpdateProvisionedModelThroughput",
    "bedrock:ApplyGuardrail",
    "bedrock:InvokeModel",
    "bedrock:InvokeModelWithResponseStream"
],
"Resource": "*"
```

THE SCOPING CATCH

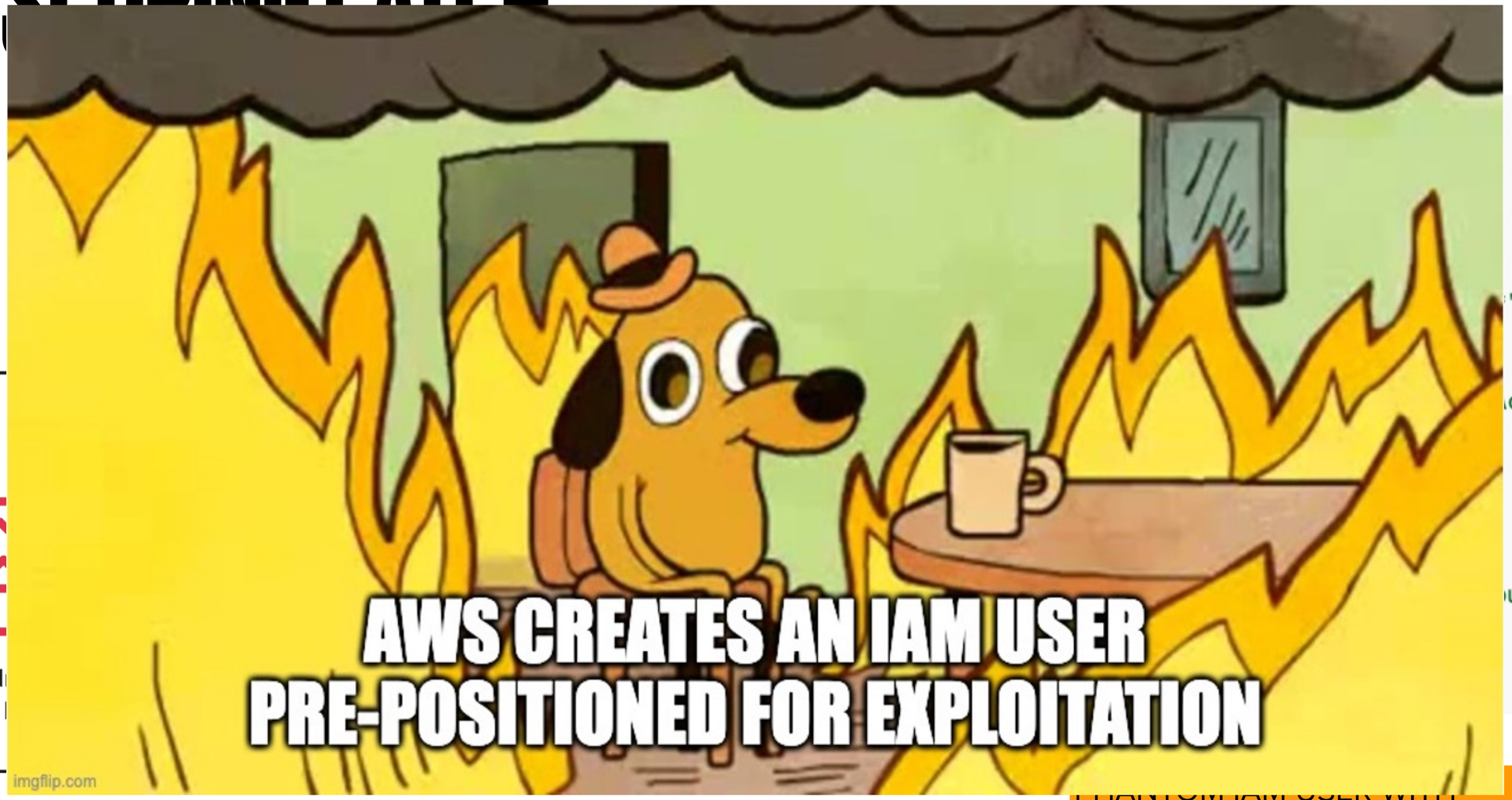


AWS SCOPED THE KEY.
THEY DIDN'T SCOPE THE USER!

```
{
    "Sid": "DescribeKey",
    "Effect": "Allow",
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "arn:*:kms:*:::*"
},
{
    "Sid": "APIsWithAllResourceAccess",
    "Effect": "Allow",
    "Action": [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
    ],
    "Resource": "*"
},
```

PHANTOM IAM USER WITH
IAM/VPC/KMS RECON CAPABILITIES

THE SCORING CATCH



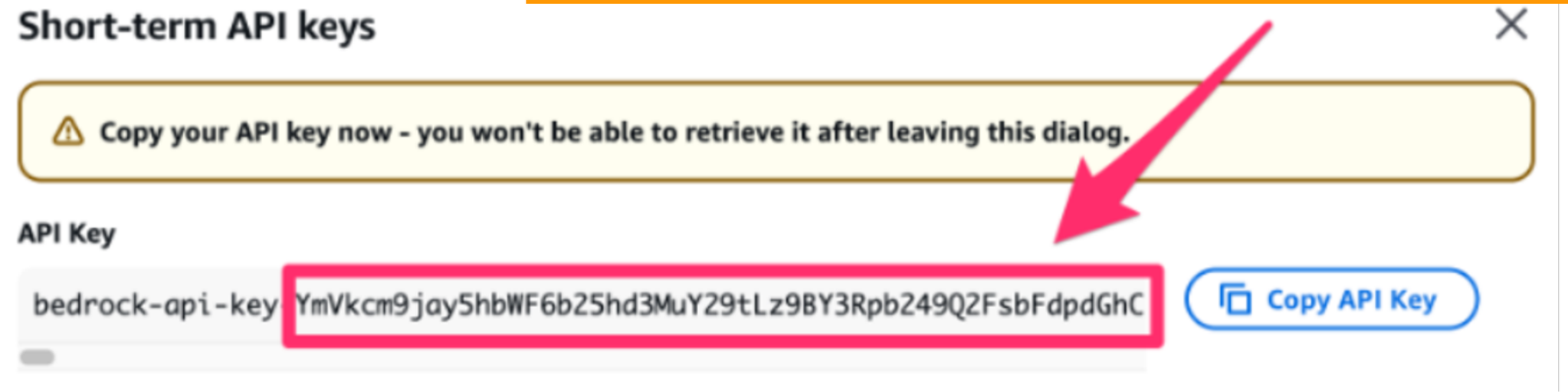
IAM/VPC/KMS RECON CAPABILITIES

DECODING THE KEYS

SHORT-TERM KEY DECODED

```
~ ❯ base64 -d
```

```
bedrock-api-key-<base64-encoded SigV4 pre-signed URL>
```



SHORT-TERM KEY DECODED

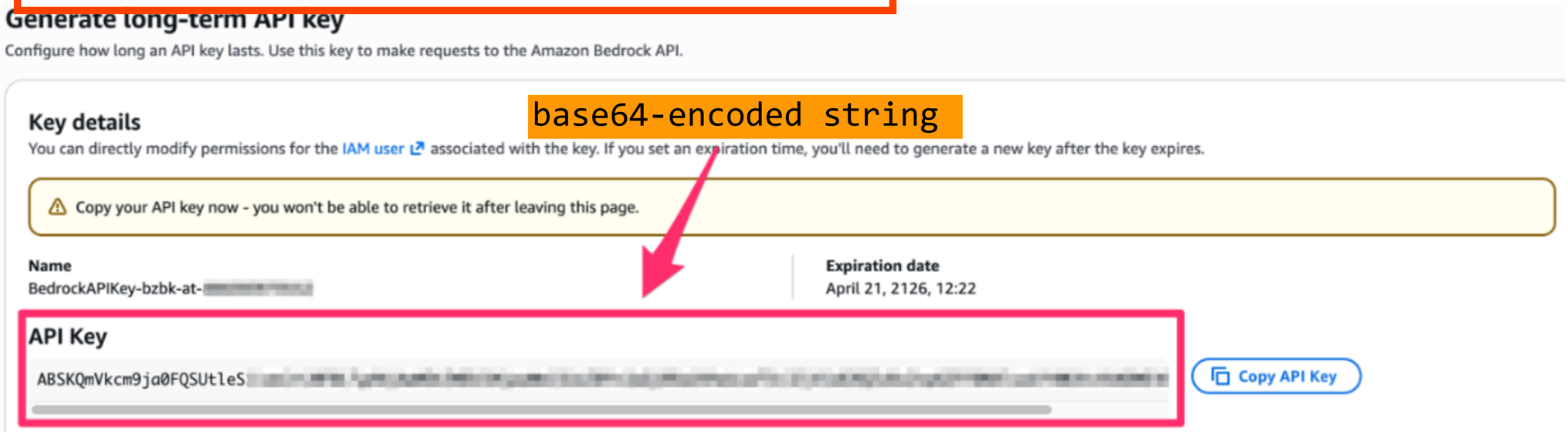
```
bedrock.amazonaws.com/?Action=CallWithBearerToken
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=<AccessKeyID>/<region>/bedrock/aws4_request
&X-Amz-Date=20260126T172726Z
&X-Amz-Expires=43200 (12 hours)
&X-Amz-Security-Token=<base64-encoded security token> → Account ID
&X-Amz-Signature=<Signature>
&X-Amz-SignedHeaders=host
&Version=1
```

LONG-TERM KEY DECODED

API Key Name

```
BedrockAPIKey-<short_id>-at-<aws_account_id>:<base64-encoded cryptographic secret>
```

```
~ ❯ base64 -d
```

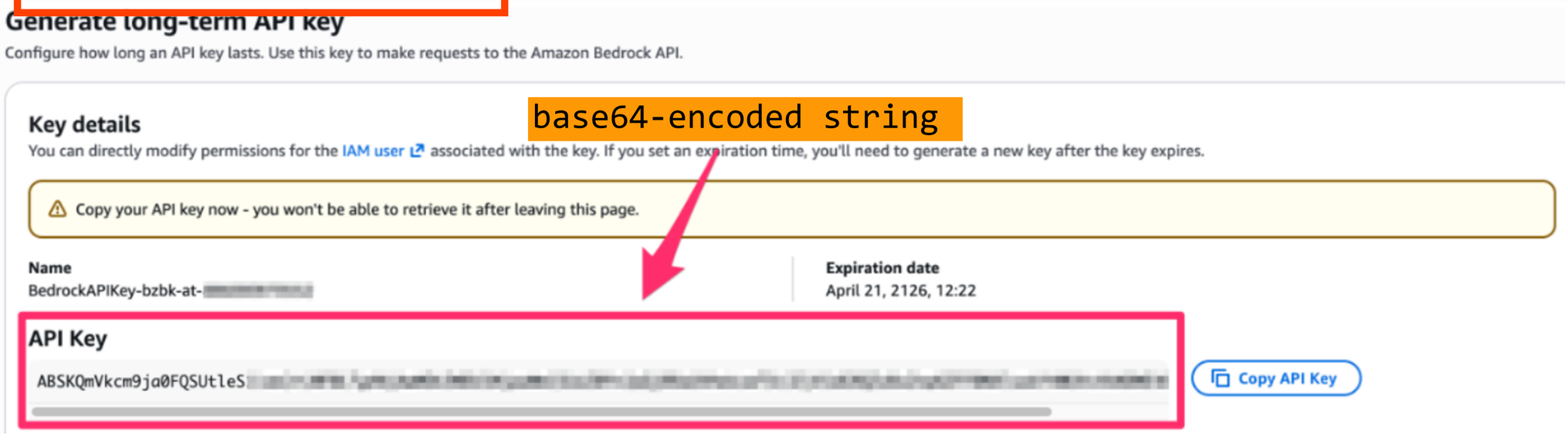


LONG-TERM KEY DECODED

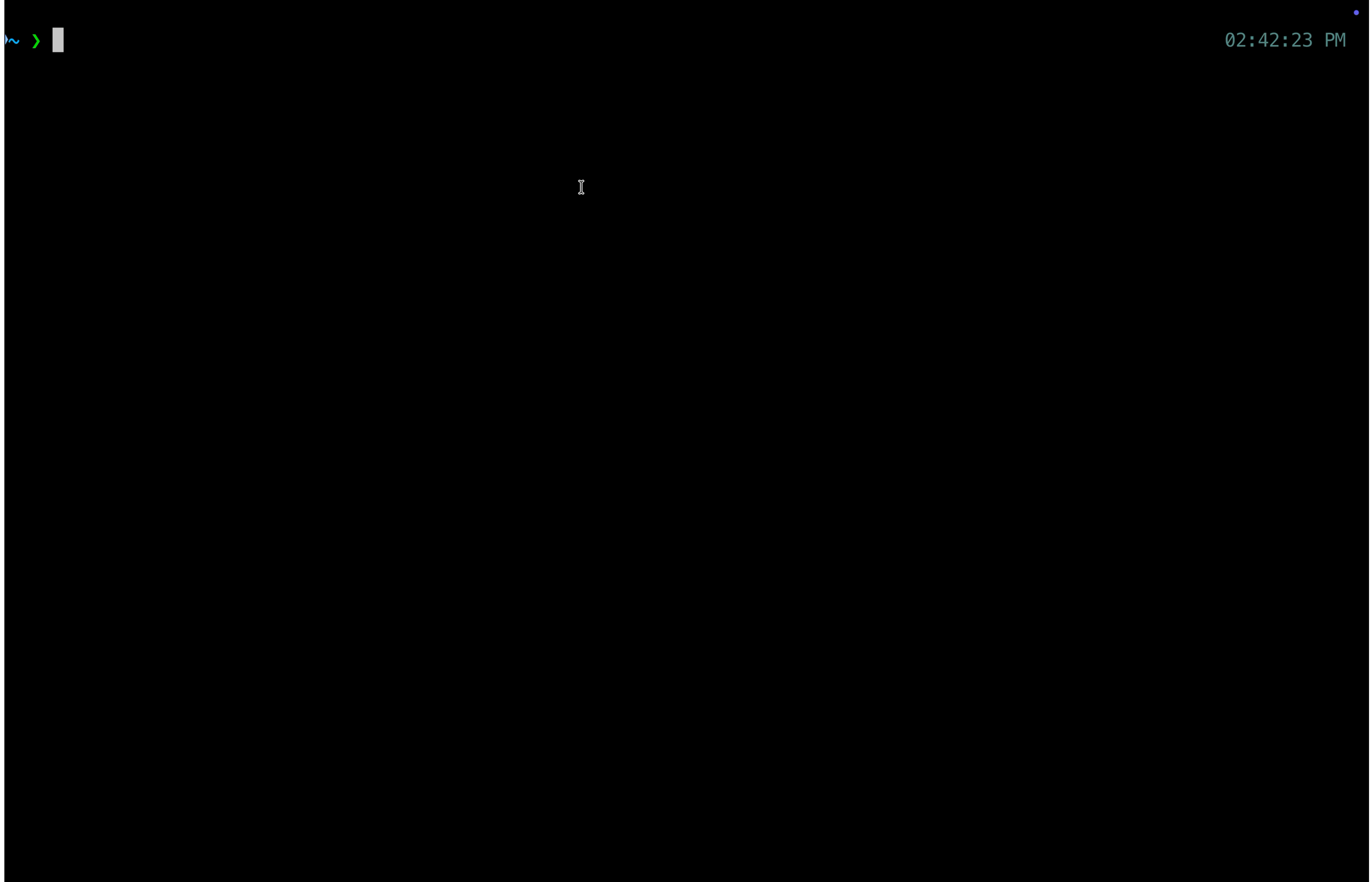
Phantom User Name

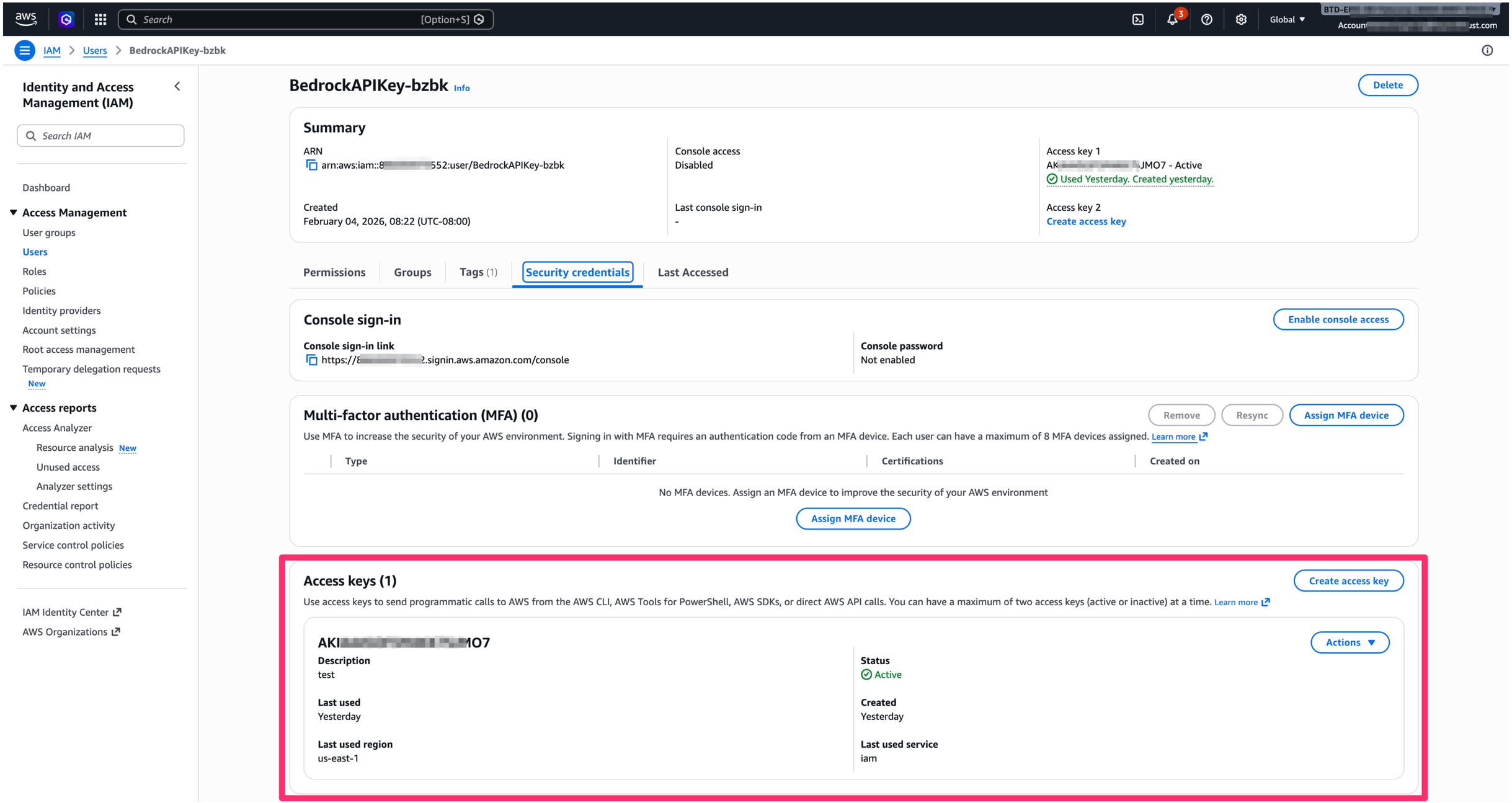
```
BedrockAPIKey-<short_id>-at-<aws_account_id>:<base64-encoded cryptographic secret>
```

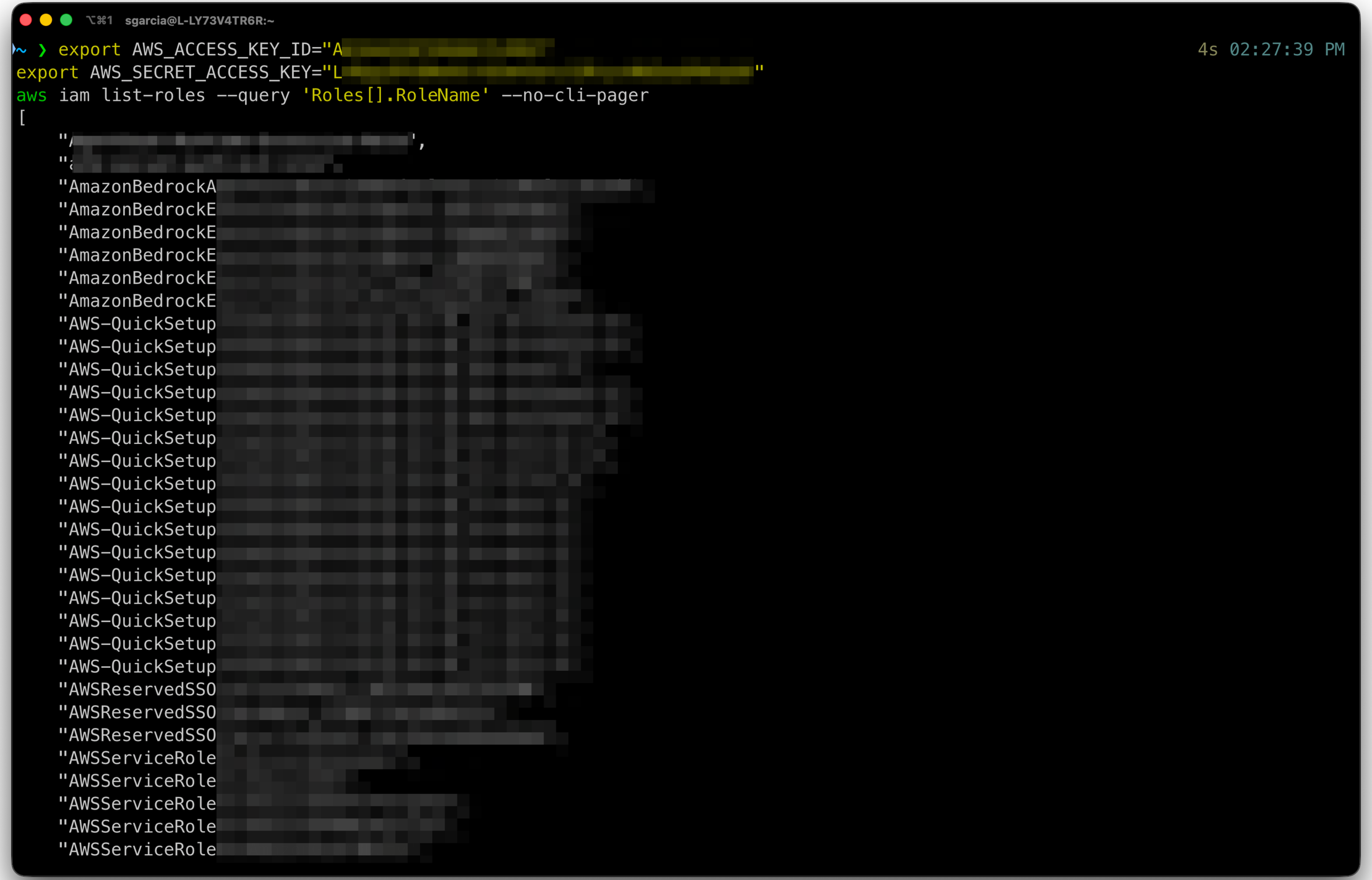
```
~ ❯ base64 -d
```



DEMO

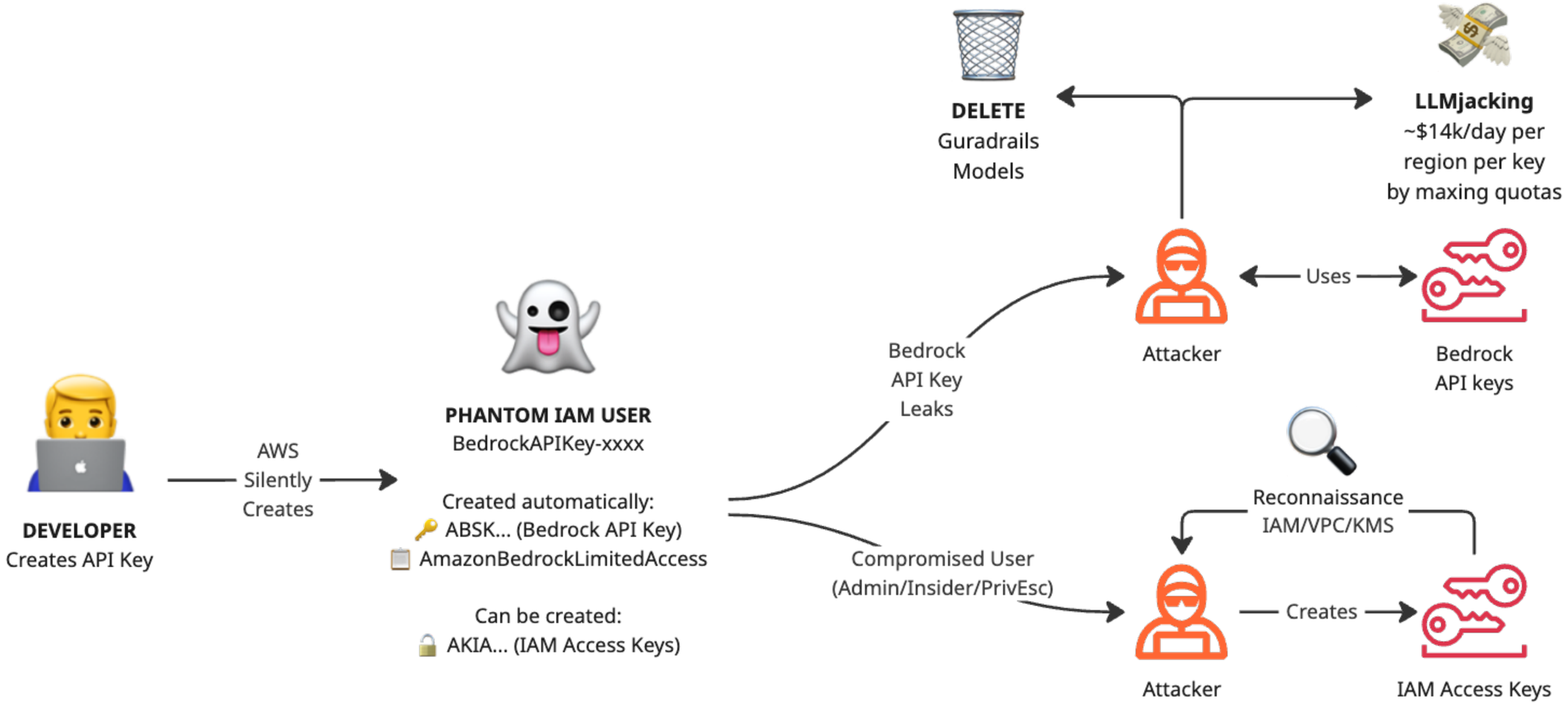

~ ❯
02:42:23 PM


Search
[Option+S]
Global
IAM > Users > BedrockAPIKey-bzbk
Identity and Access Management (IAM)
Search IAM
Dashboard
Access Management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
BedrockAPIKey-bzbk Info
Delete
Summary
ARN
arn:aws:iam::8 552:user/BedrockAPIKey-bzbk
Console access
Disabled
Access key 1
AK JMO7 - Active
Used Yesterday. Created yesterday.
Created
February 04, 2026, 08:22 (UTC-08:00)
Last console sign-in
-
Access key 2
Create access key
Permissions
Groups
Tags (1)
Security credentials
Last Accessed
Console sign-in
Enable console access
Console sign-in link
https://8 2.signin.aws.amazon.com/console
Console password
Not enabled
Multi-factor authentication (MFA) (0)
Remove
Resync
Assign MFA device
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Type
Identifier
Certifications
Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment
Assign MFA device
Access keys (1)
Create access key
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more
AKI MO7
Actions
Description
test
Status
Active
Last used
Yesterday
Created
Yesterday
Last used region
us-east-1
Last used service
iam

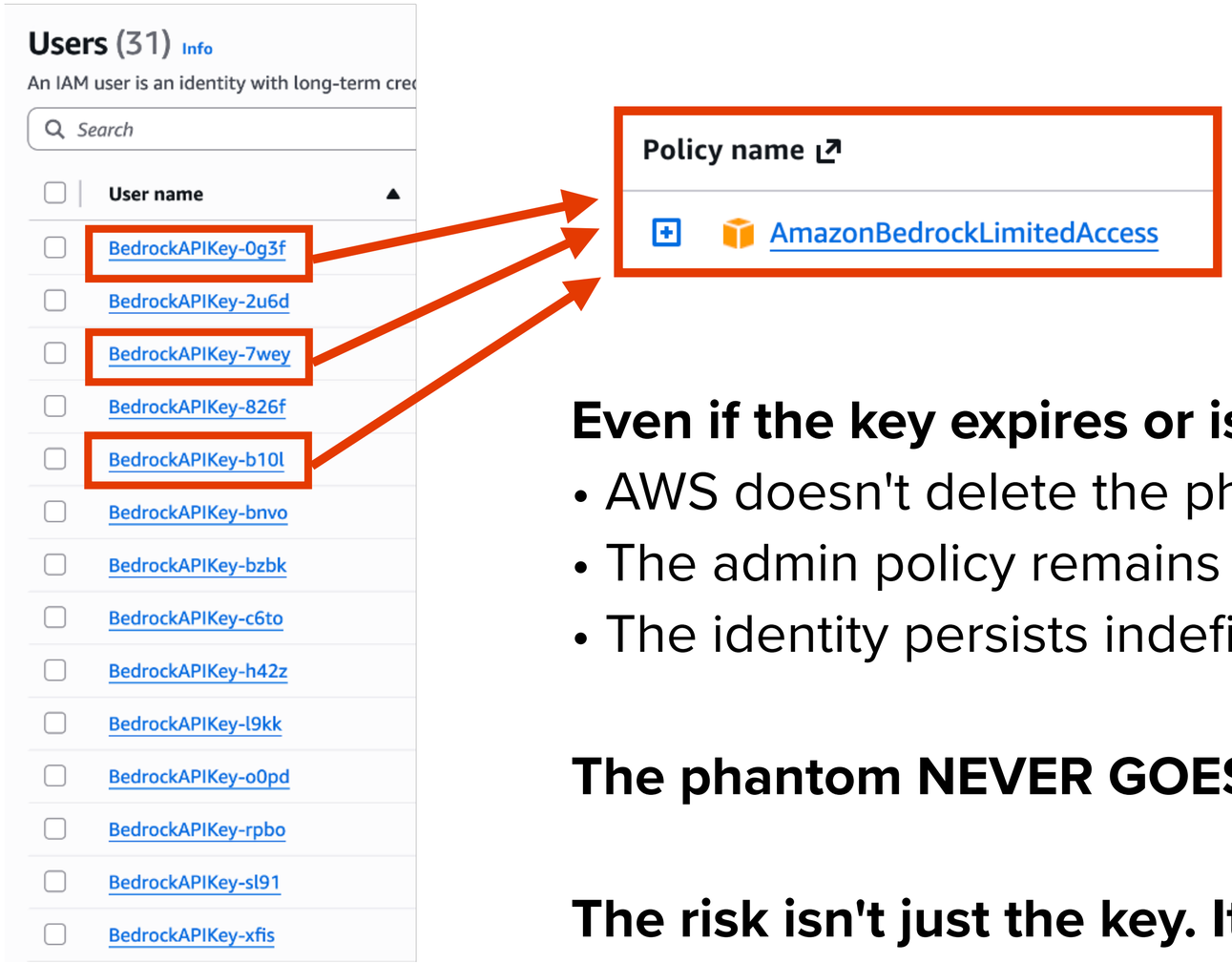

⌥⌘1 sgarcia@L-LY73V4TR6R:~
~ ❯ export AWS_ACCESS_KEY_ID="A
4s 02:27:39 PM
export AWS_SECRET_ACCESS_KEY="L
aws iam list-roles --query 'Roles[].RoleName' --no-cli-pager
[
"AmazonBedrockA
"AmazonBedrockE
"AmazonBedrockE
"AmazonBedrockE
"AmazonBedrockE
"AmazonBedrockE
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWS-QuickSetup
"AWSReservedSSO
"AWSReservedSSO
"AWSReservedSSO
"AWSServiceRole
"AWSServiceRole
"AWSServiceRole
"AWSServiceRole
"AWSServiceRole

ATTACK SCENARIOS

THE ATTACK CHAIN (LONG-TERM KEYS)



THE PHANTOM USER IS ALWAYS THERE



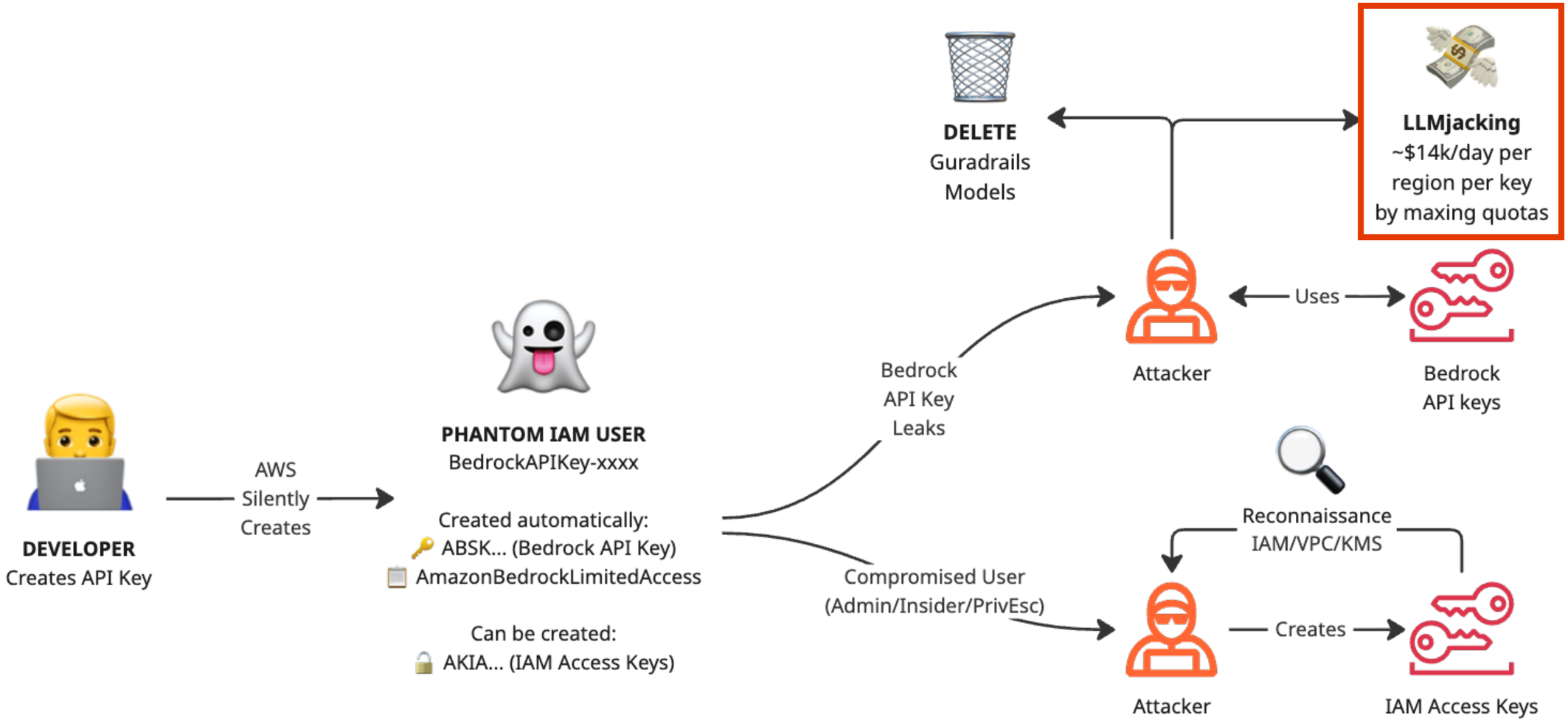
Even if the key expires or is deleted:

- AWS doesn't delete the phantom IAM user
- The admin policy remains attached
- The identity persists indefinitely until you delete it

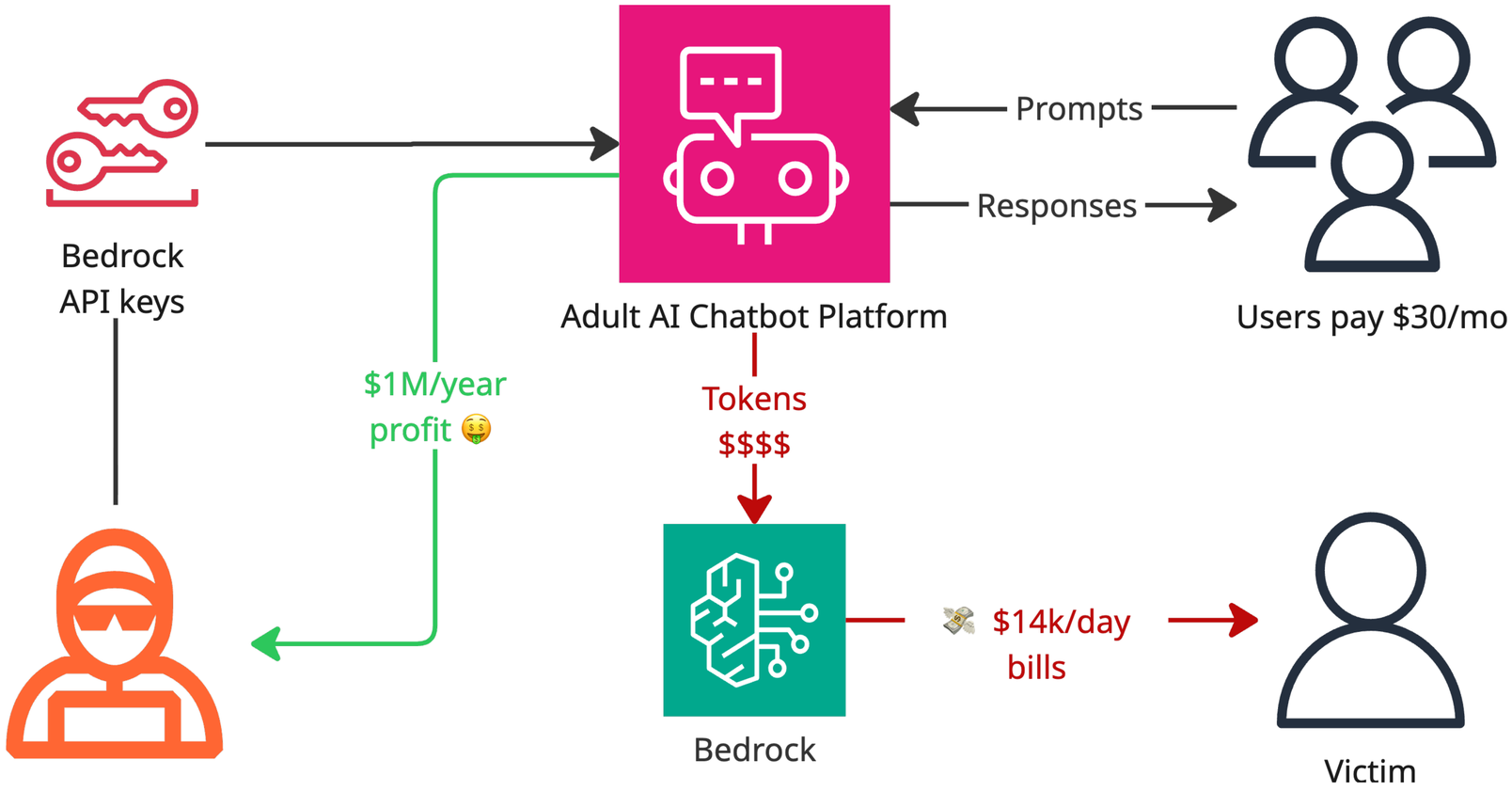
The phantom NEVER GOES AWAY!!

The risk isn't just the key. It's the permanent identity.

THE ATTACK CHAIN (LONG-TERM KEYS)



REAL-WORLD: LLMJACKING



DETECTIONS

THE ONE FIELD THAT MATTERS


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA4[redacted]7SYY",
        "arn": "arn:aws:iam::[redacted]:user/BedrockAPIKey-826f",
        "accountId": "[redacted]",
        "userName": "BedrockAPIKey-826f"
    },
    "eventTime": "2026-02-05T16:25:10Z",
    "eventSource": "bedrock.amazonaws.com",
    "eventName": "ListFoundationModels",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "104.28.237.80",
    "userAgent": "curl/8.7.1",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "callWithBearerToken": true
    },
    "requestID": "fc3e1810-9971-4797-95c0-ef03d8a24da2",
    "eventID": "4af17c7a-a1a4-429b-998d-5ac08b3456b8",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "8[redacted]",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "bedrock.us-east-1.amazonaws.com"
    }
}
```

THE ONE FIELD THAT MATTERS


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA4[redacted]7SYY",
        "arn": "arn:aws:iam::[redacted]:user/BedrockAPIKey-826f",
        "accountId": "[redacted]",
        "userName": "BedrockAPIKey-826f"
    },
    "eventTime": "2026-02-05T16:25:10Z",
    "eventSource": "bedrock.amazonaws.com",
    "eventName": "ListFoundationModels",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "104.28.237.80",
    "userAgent": "curl/8.7.1",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "callWithBearerToken": true
    },
    "requestID": "fc3e1810-9971-4797-95c0-ef03d8a24
    "eventID": "4af17c7a-a1a4-429b-998d-5ac08b3456b
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "8[redacted]",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "bedrock.us-east-1.amazonaws.com"
    }
}
```


`additionalEventData.callWithBearerToken = true`

THIS SHOWS UP WHENEVER ANY BEDROCK API KEY IS USED.

LONG-TERM? ✓
SHORT-TERM? ✓

IF YOU'RE NOT ALERTING ON THIS, START NOW.

WHAT TO MONITOR IN CLOUDTRAIL

🔑 **Long-Term Key creation:**

```
CreateServiceSpecificCredential AND serviceName = bedrock.amazonaws.com
(AND expirationDate > 90)
```

👻 **Phantom user creation:**

```
CreateUser AND userName starts with BedrockAPIKey-*
```

🎯 **Any Key Usage:**

```
additionalEventData.callWithBearerToken = true
```

🔓 **Access key creation in Phantom User:**

```
CreateAccessKey AND userName starts with BedrockAPIKey-
```

DEFENSE

SCPS ARE YOUR FRIEND

Block key creation and usage

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"DenyBedrockShortAndLongTermAPIKeys",
      "Effect": "Deny",
      "Action": [
        "iam:CreateServiceSpecificCredential",
        "bedrock:CallWithBearerToken"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Block long-term only (NEW Sept 2025)

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "bedrock:CallWithBearerToken",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "bedrock:bearerTokenType": "LONG_TERM"
                }
            }
        }
    ]
}
```

SCPS ARE YOUR FRIEND

Block creating long-term keys expiring after more than 90 days (NEW Sept 2025)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyBedrockKeysOver90Days",
      "Effect": "Deny",
      "Action": "iam:CreateServiceSpecificCredential",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:ServiceSpecificCredentialServiceName": "bedrock.amazonaws.com"
        },
        "NumericGreaterThan": {
          "iam:ServiceSpecificCredentialAgeDays": "90"
        }
      }
    }
  ]
}
```

IAM access keys for phantom BedrockAPIKey-* users

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessKeysForBedrockPhantomUsers",
      "Effect": "Deny",
      "Action": "iam:CreateAccessKey",
      "Resource": "arn:aws:iam::*:user/BedrockAPIKey-*"
    }
  ]
}
```

IR - LONG-TERM KEY COMPROMISED

Fastest: Deny the action (works immediately)

```
aws iam put-user-policy --user-name BedrockAPIKey-826f \
--policy-name DenyBedrockKey \
--policy-document '{
  "Statement": [{
    "Effect": "Deny",
    "Action": "bedrock:CallWithBearerToken",
    "Resource": "*"
  }]
}'
```

```
~ $ curl --request POST \
>   --url "https://bedrock-runtime.us-east-1.amazonaws.com/model/anthropic.claude-3-5-haiku-20241022-v1:0/converse" \
>   --header "Authorization: Bearer ${BEDROCK_API_KEY}" \
>   --header "Content-Type: application/json" \
>   --data '{
>     "messages": [{"role": "user", "content": [{"text": "Hello"}]}]
>   }'
{"Message":"User: arn:aws:iam::886000970552:user/BedrockAPIKey-826f is not authorized to perform: bedrock:CallWithBearerToken on resource: * with an explicit deny in an identity-based policy"}~
```

IR - LONG-TERM KEY COMPROMISED

```
~ $ aws iam list-service-specific-credentials \
>    --user-name BedrockAPIKey-826f
{
    "ServiceSpecificCredentials": [
        {
            "UserName": "BedrockAPIKey-826f",
            "Status": "Active",
            "ServiceCredentialAlias": "BedrockAPIKey-826f-at-8[redacted]2",
            "CreateDate": "2026-02-05T16:10:40+00:00",
            "ExpirationDate": "2026-02-06T16:10:40+00:00",
            "ServiceSpecificCredentialId": "ACCA4[redacted]",
            "ServiceName": "bedrock.amazonaws.com"
        }
    ],
    "IsTruncated": false
}
```

IR - LONG-TERM KEY COMPROMISED

```
~ $ aws iam update-service-specific-credential \
>    --user-name BedrockAPIKey-826f \
>    --service-specific-credential-id ACCA44SOF5M4JZJMXK7AZ \
>    --status Inactive
~ $
```

```
~ $ curl --request POST \
>   --url "https://bedrock-runtime.us-east-1.amazonaws.com/model/anthropic.claude-3-5-haiku-20241022-v1:0/converse" \
>   --header "Authorization: Bearer ${BEDROCK_API_KEY}" \
>   --header "Content-Type: application/json" \
>   --data '{
>     "messages": [{"role": "user", "content": [{"text": "Hello"}]}]
>   }'
{"Message":"Authentication failed: Please make sure your API Key is valid."}~ $
```

IR - LONG-TERM KEY COMPROMISED

```
~ $ aws iam delete-service-specific-credential \
>    --user-name BedrockAPIKey-826f \
>    --service-specific-credential-id ACCA[redacted]
```

```
~ $ curl --request POST \
>   --url "https://bedrock-runtime.us-east-1.amazonaws.com/model/anthropic.claude-3-5-haiku-20241022-v1:0/converse" \
>   --header "Authorization: Bearer ${BEDROCK_API_KEY}" \
>   --header "Content-Type: application/json" \
>   --data '{
>     "messages": [{"role": "user", "content": [{"text": "Hello"}]}]
>   }'
{"Message":"Authentication failed: Please make sure your API Key is valid."}~ $
```

IR - SHORT-TERM KEY COMPROMISED

Problem: Can't delete it (generated client-side, max 12 hours)

Option 1: Deny the action

```
aws iam put-role-policy --role-name test-sergio \
--policy-name DenyBedrockKeys \
--policy-document '{
  "Statement": [{
    "Effect": "Deny",
    "Action": "bedrock:CallWithBearerToken",
    "Resource": "*"
  }]
}'
```

IR - SHORT-TERM KEY COMPROMISED

Problem: Can't delete it (generated client-side, max 12 hours)

Option 2: Revoke the session

```
# Attach policy to the role that created the short-term key
# Replace COMPROMISE_TIME with when you detected the breach
aws iam put-role-policy --role-name test-sergio \
--policy-name RevokeOldSessions \
--policy-document '{
  "Statement": [{
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "DateLessThan": {
        "aws:TokenIssueTime": "2026-02-06T15:30:00Z"
      }
    }
  }]
```

DON'T WAIT 12 HOURS!!

THIS INVALIDATES ALL SESSIONS CREATED BEFORE THAT TIME.

THE TOOLKIT

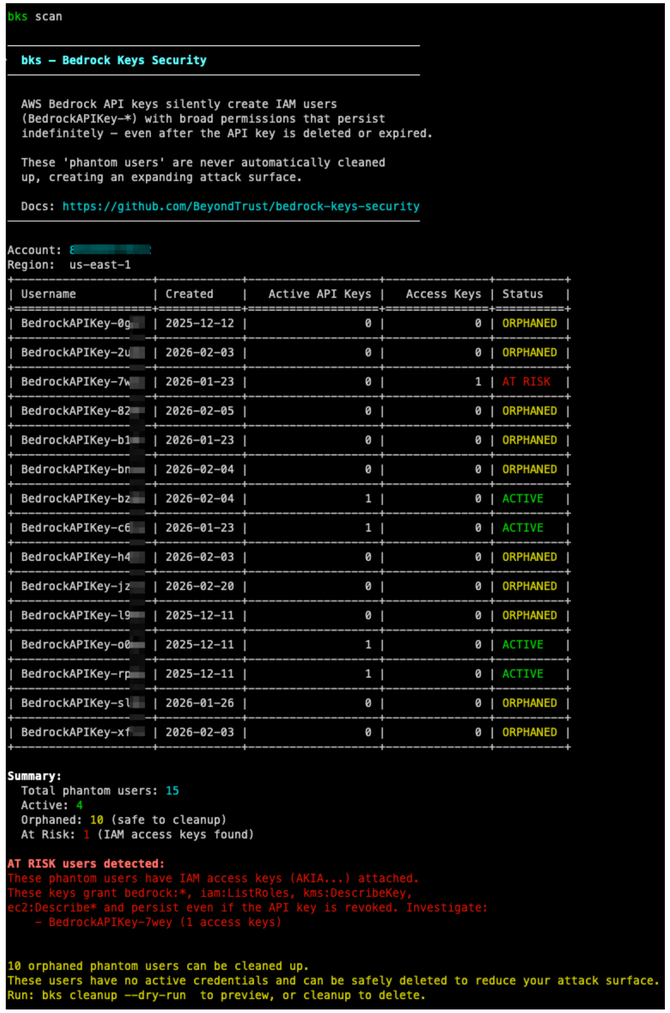
github.com/BeyondTrust/bedrock-keys-security

- **One command finds every phantom in YOUR account:**

bks scan

Bedrock API keys Toolkit:

- Phantom User Hunter: Find BedrockAPIKey-* in your account
- Cleanup Automation: Delete orphaned phantoms safely
- Key Decoder: Extract account IDs, Usernames, regions from leaked keys
- Incident response: emergency key revocation, CloudTrail timelines, and forensic reports.
- 4 Ready-to-Deploy SCPs: Block creation, enforce limits



MONDAY MORNING CHECKLIST

github.com/BeyondTrust/bedrock-keys-security



1. Find phantom users in YOUR account

```
bks scan
```

```
OR manually:
```

```
aws iam list-users | grep BedrockAPIKey
```

2. Deploy detection in your SIEM

- Monitor CloudTrail for `callWithBearerToken = true`
- Alert on `CreateUser with BedrockAPIKey-*`
- Alert on `CreateAccessKey` for phantom users

3. Block them if you don't need API keys

```
# SCP to deny creation and usage
```

```
iam:CreateServiceSpecificCredential AND
bedrock:CallWithBearerToken
```

4. If you DO need them:

- Max 90-day expiry (use condition key)
- Monitor closely
- Rotate frequently

DON'T WAIT FOR THE $14K SURPRISE !!

TAKEAWAYS

- **AWS creates phantom IAM users →** buried in CloudTrail, not truly invisible
- **"Limited" is marketing →** ADMIN Bedrock perms + IAM/VPC/KMS recon!
- **Keys leaked in 2 weeks, already weaponized →** $14k/day regional damage, $1M/year criminal revenue
- **The phantom user is always at risk →** credential leaks, insider threats, privilege escalation

ADDITIONAL RESOURCES

- https://docs.aws.amazon.com/bedrock/latest/userguide/api-keys-permissions.html
- https://aws.amazon.com/blogs/security/securing-amazon-bedrock-api-keys-best-practices-for-implementation-and-management/
- https://aws.amazon.com/blogs/machine-learning/accelerate-ai-development-with-amazon-bedrock-api-keys/
- https://github.com/aws-samples/aws-customer-playbook-framework/blob/main/detections/Bedrock_Api_Key_Eventbridge_Detection.md
- https://github.com/aws-samples/service-control-policy-examples/tree/main/Service-specific-controls/Amazon-Bedrock

THANK YOU!

Sergio Garcia
Security Researcher @ BeyondTrust

Twitter: @MrCloudSec
LinkedIn: linkedin.com/in/MrCloudSec
GitHub: github.com/MrCloudSec

github.com/BeyondTrust/bedrock-keys-security



Track 1 Survey: