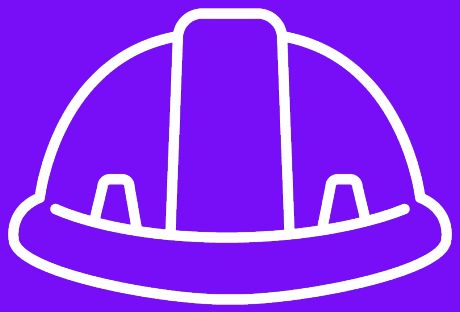
AWS Identity and Access Management (IAM): IAM Roles

Andru Estes
Principal Author
andru-estes

What Are IAM Roles?



IAM Roles

Another type IAM identity that you create in your account that has specific permissions

Important IAM Role Concepts

Similar to IAM Users, except these can be assumed by whoever needs access

No long-term credentials used! Credentials are temporary and rolling.

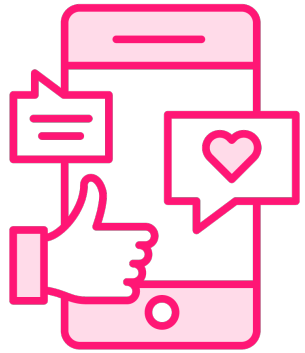
Useful for delegating access to many users, apps, or services

Control permissions and access via permissions policies and trust policies

IAM Role Types

Service-linked Roles
Allow AWS services to access AWS resources securely

Instance Profiles
Attached to EC2 instances to allow use of the IAM Role



Federated Identities
Allows external identities (*e.g. Google*) to assume roles

Three Common Use Cases for IAM Roles

Grant access to Lambda functions to allow them to access AWS resources like DynamoDB

Grant access to EC2 instances to allow them to interact with services like Amazon S3

Set up a role to allow cross-account access from another AWS account for third-party vendors

AWS Security Token Service (STS)

AWS STS is the backbone for how IAM Roles generate their credentials!

Service that enables you to request short-term, temporary credentials for users

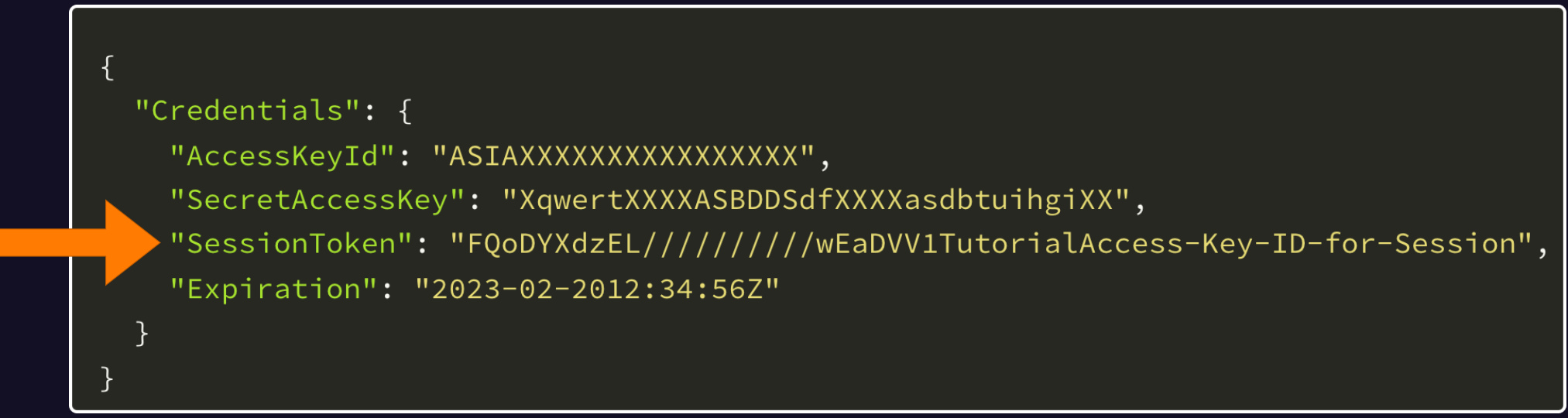
Credentials can be set to last as little as 15 minutes, or as long as 12 hours

Commonly used with SAML federation and OIDC* federation

Supports requirements for MFA and other conditional access

** OpenID Connect*

IAM Role Session Credentials



Assuming and using an IAM Role **REQUIRES** a Session Token be present

IAM Role Trust Policies

IAM Role Trust Policies

Resource-based JSON document

Define which principals are trusted to assume the role

Principals can be IAM users, IAM roles, AWS accounts, and AWS services

They are required for a role to be usable

Trust Policy Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/cloud_user"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

The Principal that can assume the role

Trust Policy Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/cloud_user"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

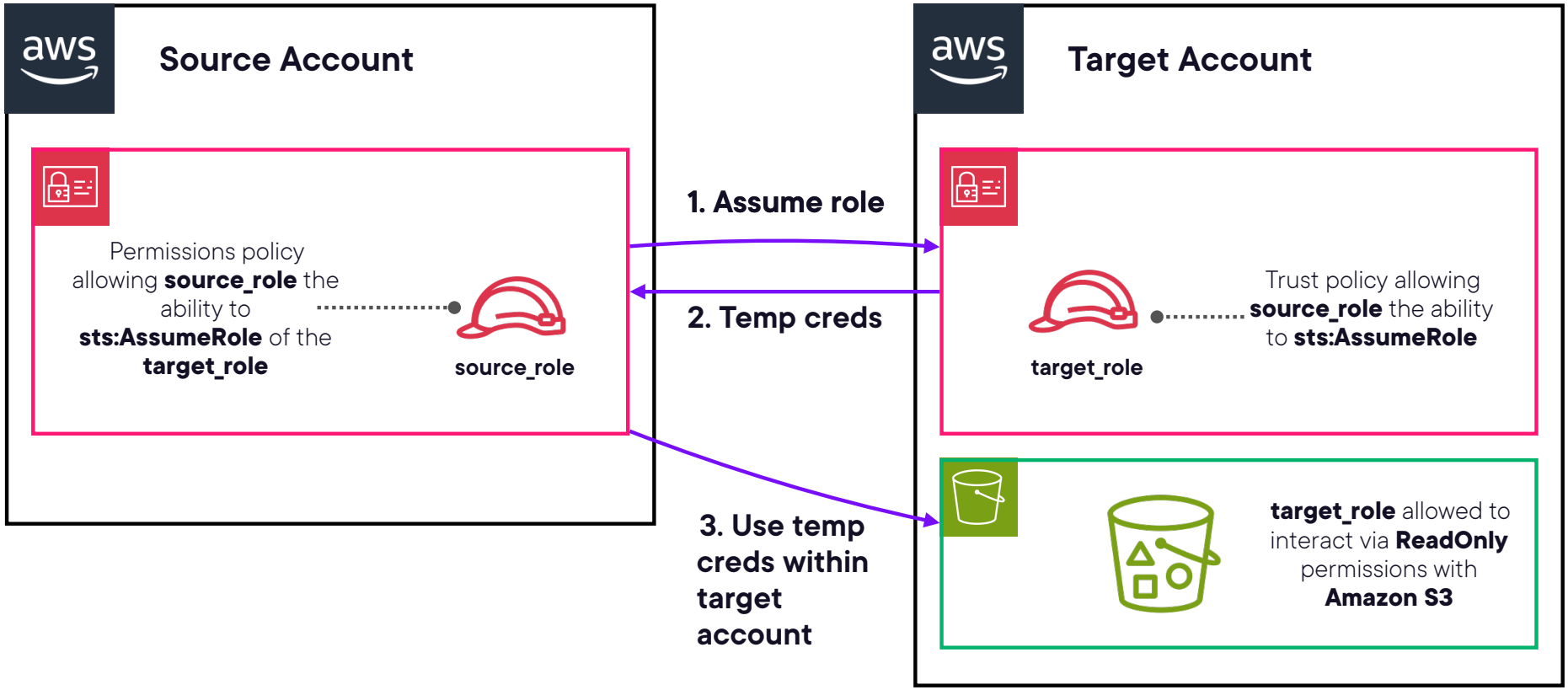
The API Action being called

Trust Policy Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/cloud_user"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

Any conditions you may want to include

Demo: Creating a Cross-account IAM Role



EC2 Instance Profiles

EC2 Instance Profiles

Use these to pass an IAM role to an EC2 instance

Creating a role for Amazon EC2 in console results in automatic instance profile creation

The list of IAM roles when creating an EC2 instance is actually a list of instance profiles

These are required for leveraging IAM role credentials with EC2 instances

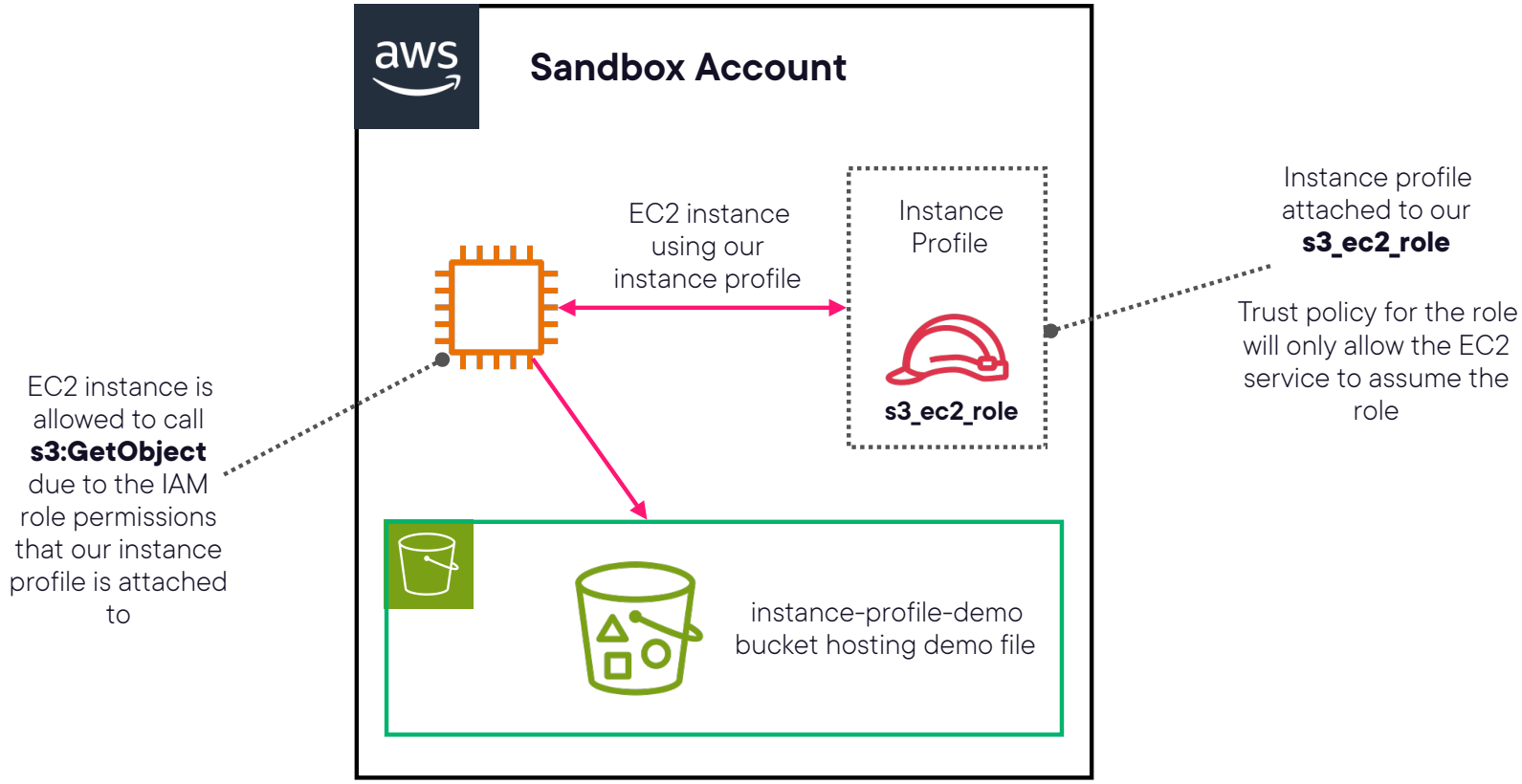
Instance profiles are required to pass IAM role credentials to EC2 instances due to how the hypervisor works!

Instance Profile Use Cases

Application running on EC2 that needs to access Amazon S3 for storing documents

Message polling application running on EC2 which needs to pull messages off an SQS queue

Demo: Creating an EC2 Instance Profile



Module Summary and Exam Tips

AWS IAM Roles

IAM role offer an assumable IAM entity for performing AWS actions

Roles leverage temporary credentials to grant access

AWS Security Token Service (STS) is the backbone to IAM role credentials

You should always leverage IAM roles whenever possible!

Remember Three Common Use Cases for IAM Roles

Grant access to Lambda functions to allow them to access AWS resources like DynamoDB

Grant access to EC2 instances to allow them to interact with services like Amazon S3

Set up a role to allow cross-account access from another AWS account for third-party vendors

IAM Role Trust Policies

Define which principals are trusted to assume the role

Required to actually assume an IAM role

Trust Policy Example

You need to know how to read a trust policy!

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/cloud_user"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

EC2 Instance Profiles are attached to IAM roles, and allow the EC2 instances to obtain the role credentials!