Rouble Malik

Feb 2 · 6 min read · Listen

Introduction to AWS IAM AssumeRole

Before we jump right into the concept of IAM AssumeRole, it is important to understand the fundamentals.

Please allow me to dissect this topic into three sub-topics:

1. What is an IAM user?
2. What is an IAM Role
3. What is an AssumeRole?

What is an IAM user?

An AWS Identity and Access Management (IAM) *user* is an entity that you create in AWS. The IAM user represents the human user or workload who uses the IAM user to interact with AWS Services. A user in AWS consists of a name and credentials.

By default, a new IAM user has no permissions to do anything. A set of permissions needs to be assigned to the user which defines what the user is allowed to do and not do. Basically

What is an IAM role?

An IAM (Identity and Access Management) role is an AWS (Amazon Web Services) entity that defines a set of permissions for making AWS service requests. An IAM role can be assumed by AWS services, applications running on Amazon EC2 instances, and AWS Identity and Access Management (IAM) users. The role defines what actions can be performed and on which AWS resources. This allows fine-grained control over access to AWS resources and helps ensure the least privilege principle is followed.

What is an AssumeRole?

IAM (Identity and Access Management) AssumeRole is an AWS service that enables you to delegate access to AWS resources without sharing your AWS account root user credentials. It allows you to grant trusted users, such as IAM users, roles, or applications, the permissions to access your AWS resources. This is useful when you need to grant access to your AWS resources to a third-party application, or when you want to allow multiple people within your organization to manage different aspects of your AWS infrastructure.

Assuming a role enforces AWS Security best practices in IAM. The principal it enforces the highest is principal of least privileges. Also assuming a role provide temporary security credentials that are valid for a duration and provide a set of permissions.

A role can be assumed by:

1. An IAM user

2. Another IAM role which can be from the same AWS account or another AWS account
3. An AWS Service. For example EC2, Lambda etc.

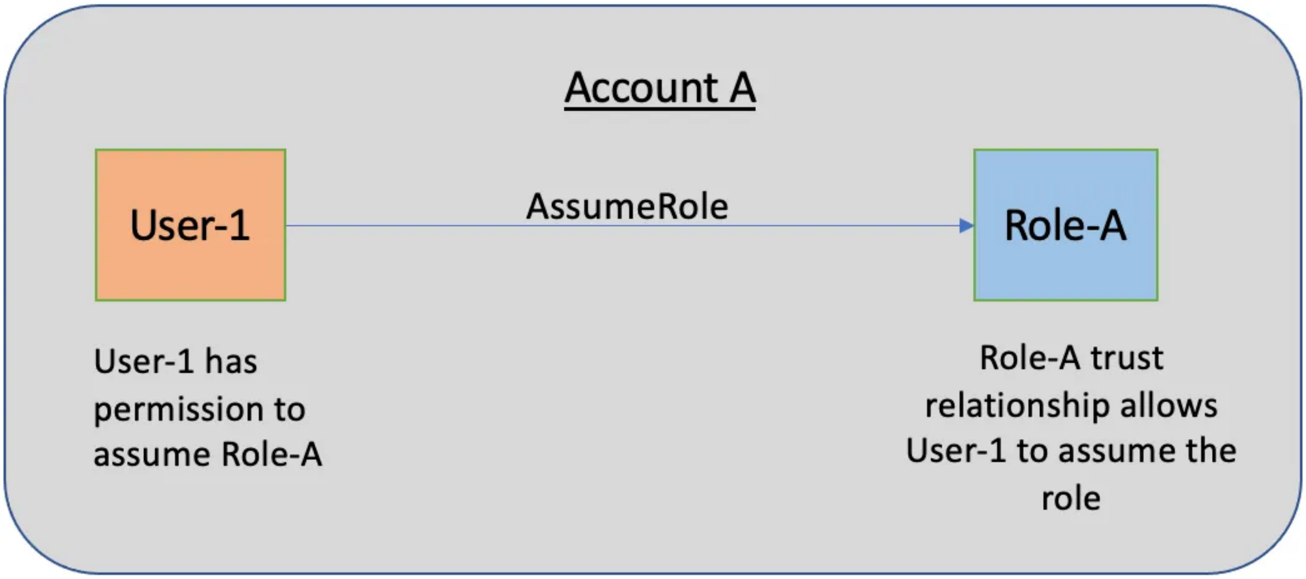
Criteria for assuming a role is:

- User/role/service must have the permissions to assume another role.
- The role trust relationship should allow the user/role/service to assume.

The role which is to be assumed can be in the same AWS account or a different AWS account.

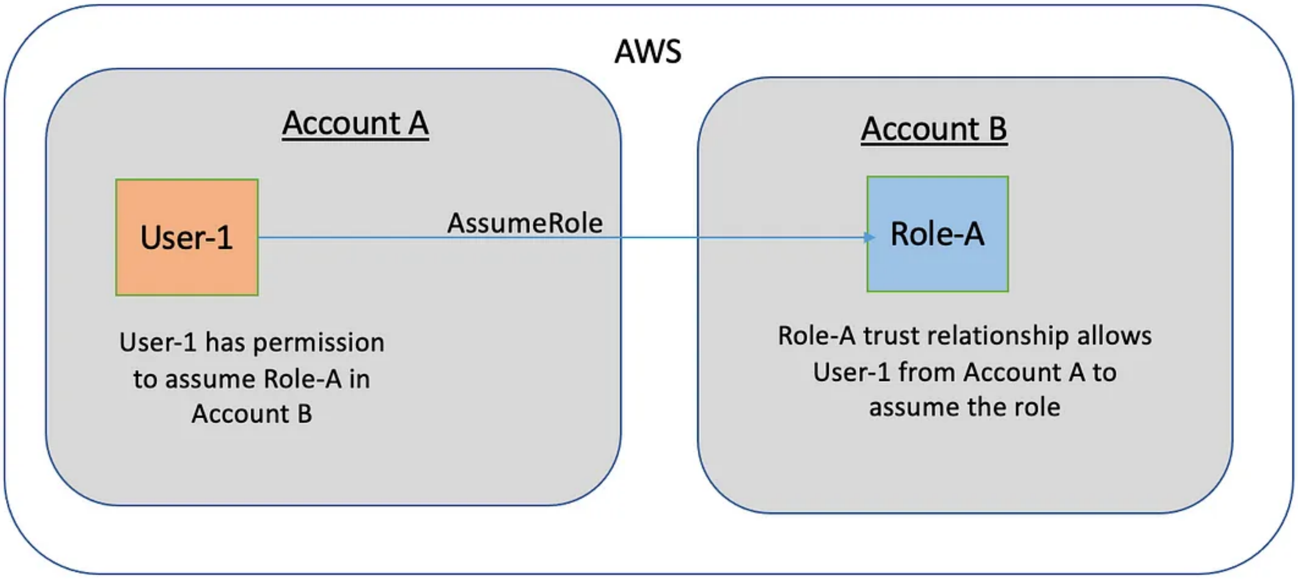
Let us now try to understand this with the help of a picture diagram, because as the saying goes "*a picture paints a thousand words*".

An IAM role assumed by an IAM user.


Account A
User-1
AssumeRole
Role-A
User-1 has permission to assume Role-A
Role-A trust relationship allows User-1 to assume the role

User-1 assumes Role-A in the same AWS account.

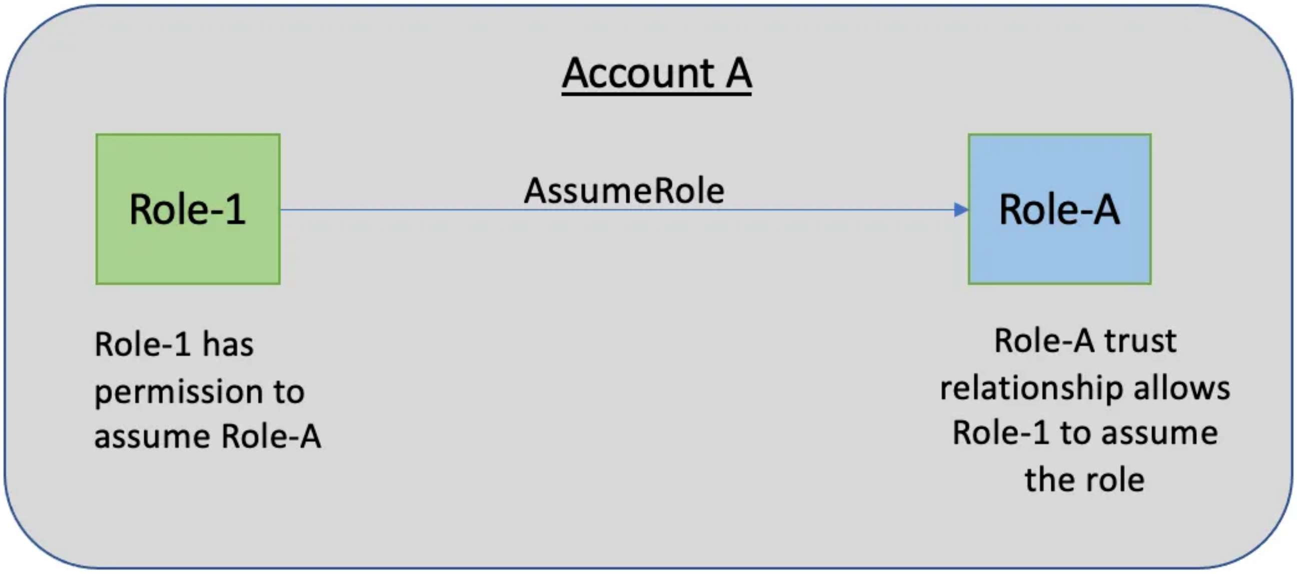
The User-1 is able to assume Role-A in the same AWS account as long as User-1 has the permissions in the IAM policy and Role-A trust relationship allows User-1 to assume the role.


AWS
Account A
User-1
AssumeRole
User-1 has permission to assume Role-A in Account B
Account B
Role-A
Role-A trust relationship allows User-1 from Account A to assume the role

User-1 assumes Role-A in a different AWS account.

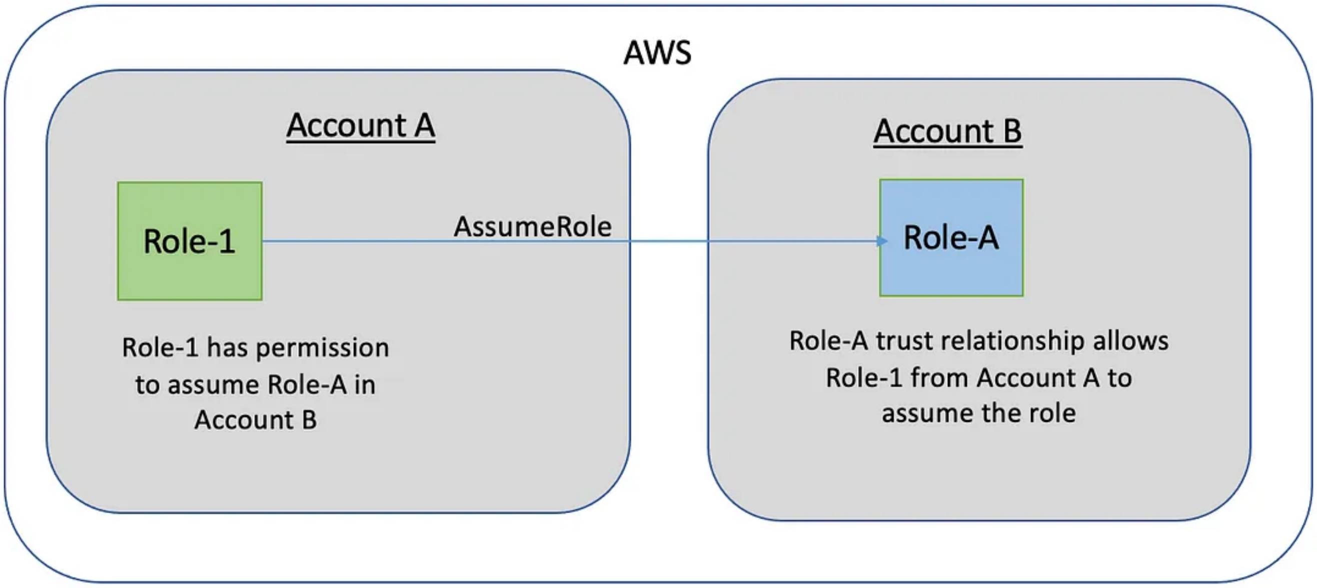
The User-1 is able to assume Role-A in a different AWS account (cross-account) as long as User-1 has the permissions in the IAM policy and Role-A trust relationship allows User-1 to assume the role.

An IAM role assumed by another IAM role.


Account A
Role-1
AssumeRole
Role-A
Role-1 has permission to assume Role-A
Role-A trust relationship allows Role-1 to assume the role

Role-1 assumes Role-A in the same AWS account.

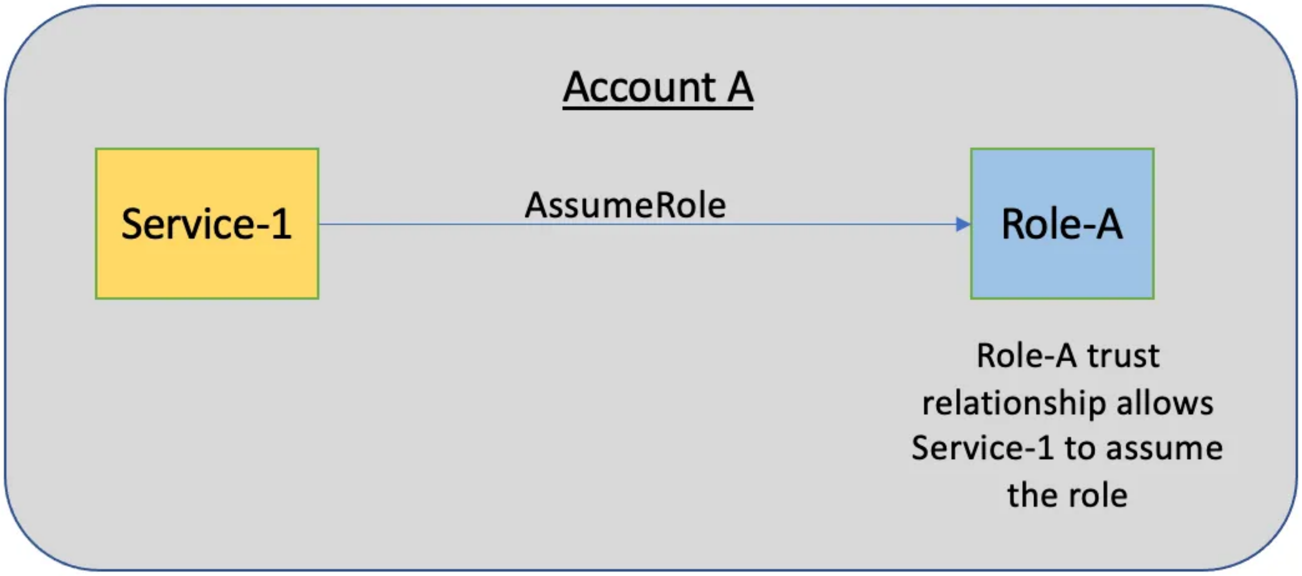
The Role-1 is able to assume Role-A in the same AWS account as long as Role-1 has the permissions in the IAM policy and Role-A trust relationship allows Role-1 to assume the role.


AWS
Account A
Role-1
AssumeRole
Role-1 has permission to assume Role-A in Account B
Account B
Role-A
Role-A trust relationship allows Role-1 from Account A to assume the role

Role-1 assumes Role-A in a different AWS account.

The Role-1 is able to assume Role-A in a different AWS account (cross-account) as long as Role-1 has the permissions in the IAM policy and Role-A trust relationship allows Role-1 to assume the role.

An IAM role assumed by AWS Service.


Account A
Service-1
AssumeRole
Role-A
Role-A trust relationship allows Service-1 to assume the role

Service-1 assumes Role-A in the same AWS account.

If Role-A trust relationship allows Service-1 to assume the role, an AWS Service such as EC2 or lambda etc can assume the role.

Let us also try to understand this practically with examples.

An IAM role assumed by an IAM user.

User-1 is in AWS account 1111111111 and wants to assume Role-A in the same AWS account. Below is the User-1 permissions to assume Role-A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "User-A assume Role-A in the same account",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::1111111111:role/Role-A"
        }
    ]
}
```

User-1 is in AWS account 1111111111 and wants to assume Role-A in a different AWS account 2222222222. Below is the User-1 permissions to assume Role-A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "User-1 assume Role-A in a different account",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::2222222222:role/Role-A"
        }
    ]
}
```

Below is the Role-A trust relationship which allows User-1 to assume the role in same AWS account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::1111111111:user/User-1"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Below is the Role-A trust relationship in AWS account 2222222222 which allows User-1 from third AWS account to assume the role (cross-account).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::3333333333:user/User-1"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

An IAM role assumed by another IAM role.

Role-1 is in AWS account 1111111111 and wants to assume Role-A in the same AWS account. Below is the Role-A permissions to assume Role-A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Role-1 assume Role-A in the same account",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::1111111111:role/Role-A"
        }
    ]
}
```

Role-1 is in AWS account 1111111111 and wants to assume Role-A in a different AWS account 2222222222. Below is the Role-1 permissions to assume Role-A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Role-1 assume Role-A in a different account",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::1111111111:role/Role-A"
        }
    ]
}
```

Below is the Role-A trust relationship which allows Role-1 to assume the role in same AWS account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::1111111111:role/Role-1"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Below is the Role-A trust relationship in AWS account 2222222222 which allows Role-1 from third AWS account to assume the role (cross-account).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::3333333333:role/Role-1"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

An IAM role assumed by AWS Service.

Below is the Role-A trust relationship which allows EC2 service to assume this role. Once you attach this role to the EC2 instance, the instance can successfully assume the role perform tasks.

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

You can assume a role using the STS AssumeRole Operation.

The assume role operation can be performed by:

1. AWS Console
2. AWS CLI
3. AWS SDK

Once you assume a role successfully, you get temporary security credentials. It consists of :

- Access Key ID
- Secret Access Key
- Security Token

If you are performing the action via AWS Console, you don't have to perform any additional step, but if you are performing AssumeRole action via CLI or SDK, you need to export the temporary security credentials in the environment to completely assume the role.

I hope you found the above information helpful. Please feel free to drop a comment or reach out if you have any questions or feedback.

References:

[1] https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html

[2] https://docs.aws.amazon.com/IAM/latest/UserGuide/access.html

[3] https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html?secd_iam7

[4] https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html

[5] https://aws.amazon.com/premiumsupport/knowledge-center/iam-assume-role-cli/