**1. What is MFA**

Multi Factor authentication (MFA) is a security system that requires more than one method of [authentication](https://searchsecurity.techtarget.com/definition/authentication) from independent categories of credentials to verify the user’s identity for a login or other transaction.

AWS Multi-Factor Authentication (MFA) is the practice or requiring two or more forms of authentication to protect AWS resources. It is an added security feature available through Amazon Identity and0xdsew566rjtt2hhhhrtrhnnrn yy Access Management (IAM) that strengthens username and password credentials.It is considered a best practice for MFA to be used for a root account or for “highly-privileged” users who have access to sensitive resources. It can be used for cross-account access across multiple AWS accounts. This is helpful if your company has multiple accounts and a trusted user needs to access all of them.

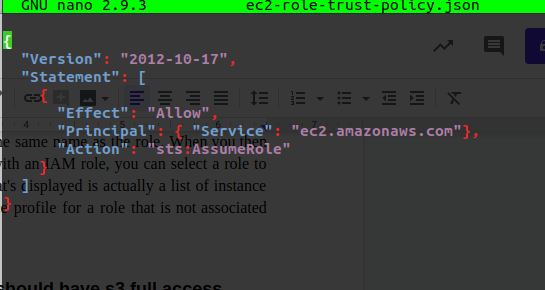
**2. What is ec2 instance profile**

An instance profile is a container for an IAM role that you can use to pass role information to an EC2 instance when the instance starts.

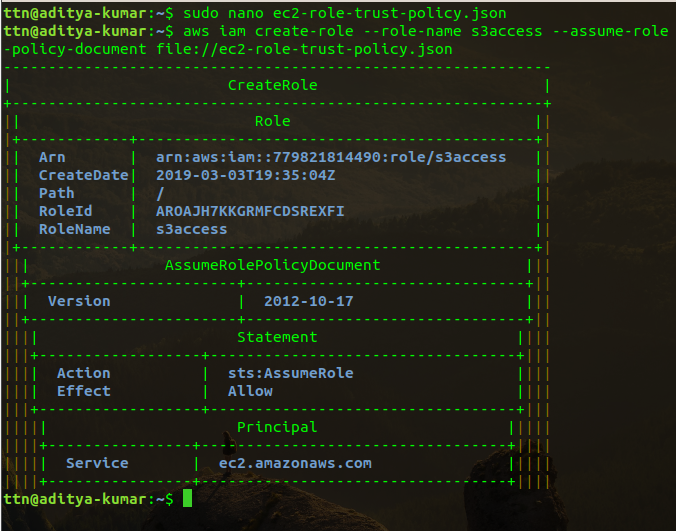
If we use the AWS Management Console to create a role for Amazon EC2, the console automatically creates an instance profile and gives it the same name as the role. When you then use the Amazon EC2 console to launch an instance with an IAM role, you can select a role to associate with the instance. In the console, the list that's displayed is actually a list of instance profile names. The console does not create an instance profile for a role that is not associated with Amazon EC2.

**3. Create a role from AWS CLI and which should have s3 full access permission and attach the role to an ec2 instance.**

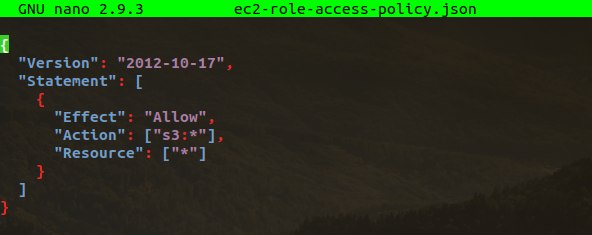
* 1. Create the following trust policy and save it in a text file named ec2-role-trust-policy.json.

****

* 1. Create the s3access role and specify the trust policy that you created.

****

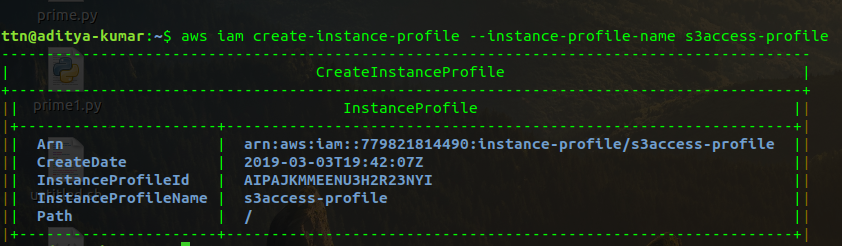
3.Create an access policy and save it in a text file named ec2-role-access-policy.json. For example, this policy grants administrative permissions for Amazon S3 to applications running on the instance.



4.Attach the access policy to the role.

****

**5.**Create an instance profile named s3access-profile.

****

**6.**Add the s3access role to the s3access-profile instance profile.

****

7.Use the [run-instances](https://docs.aws.amazon.com/cli/latest/reference/ec2/run-instances.html) command to launch an instance using the instance profile. The following example shows how to launch an instance with the instance profile.

aws ec2 run-instances --image-id ami-11aa22bb --iam-instance-profile Name="s3access-profile" --key-name my-key-pair --security-groups my-security-group --subnet-id subnet-1a2b3c4d

**4. Create a policy which should have following things:**

* **Should have a tag with name 'Owner'**
* **'Owner' tag key should have some value.**
* **The value must be equal to the username of the logged-in user.**

