AWS EC2-Instance-connect

new feature of EC2 SSH connection, **EC2 Connect**. A new way to control SSH access to your EC2 instances using **Identity and Access Management (IAM)**.

How to Configure

- Verify the general prerequisites for connecting to your instance using SSH.
  - Get information about your instance
  - Locate the private key and verify permissions
  - Enable Inbound traffic

    Ensure that the security group associated with your instance allows inbound SSH traffic on port 22 from your IP address.
- At first time, we need to install the Instance Connect on the instance. This is a one-time requirement for each instance.

  Amazon Linux 2 2.0.20190618 or later comes preconfigured with EC2 Instance Connect. For other supported Linux distributions, you must

set up Instance Connect for every instance that will support using Instance Connect.
Notes : If you configured the `AuthorizedKeysCommand` and `AuthorizedKeysCommandUser` settings for SSH authentication, the EC2 Instance Connect installation will not update them. As a result, you cannot use Instance Connect.

- (Optional) Install the EC2 Instance Connect CLI.

  `pip install ec2instanceconnectcli`
  The **EC2 Instance Connect CLI** provides a similar interface to standard SSH calls, which includes querying EC2 instance information, generating and publishing ephemeral public keys, and establishing an SSH connection through a single command.
- Connect to your instance using SSH.
- Install the EC2 Instance Connect package on your instance.
  - For **Amazon Linux 2**, use the yum install command.
    `sudo yum install ec2-instance-connect`
  - For **Ubuntu**, use the sudo apt-get command to install the .deb package
    `sudo apt-get install ec2-instance-connect`
- Configure IAM policy for EC2 Instance Connect

  For your IAM users to connect to an instance using EC2 Instance Connect, **you must grant them permission to push the public key to the instance**.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSSHPublicKey"
```

```
            ],
            "Resource": [
                "arn:aws:ec2:Your-Region-1:ACCOUNTID:instance/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ec2-user"
                }
            }
        }
    ]
}
```

You need to modify the `Your-Region-1` and `ACCOUNTID` in the policy.

- Attach the policy to IAM Group or IAM User.

  Restrict the permissions to the specific user or group.