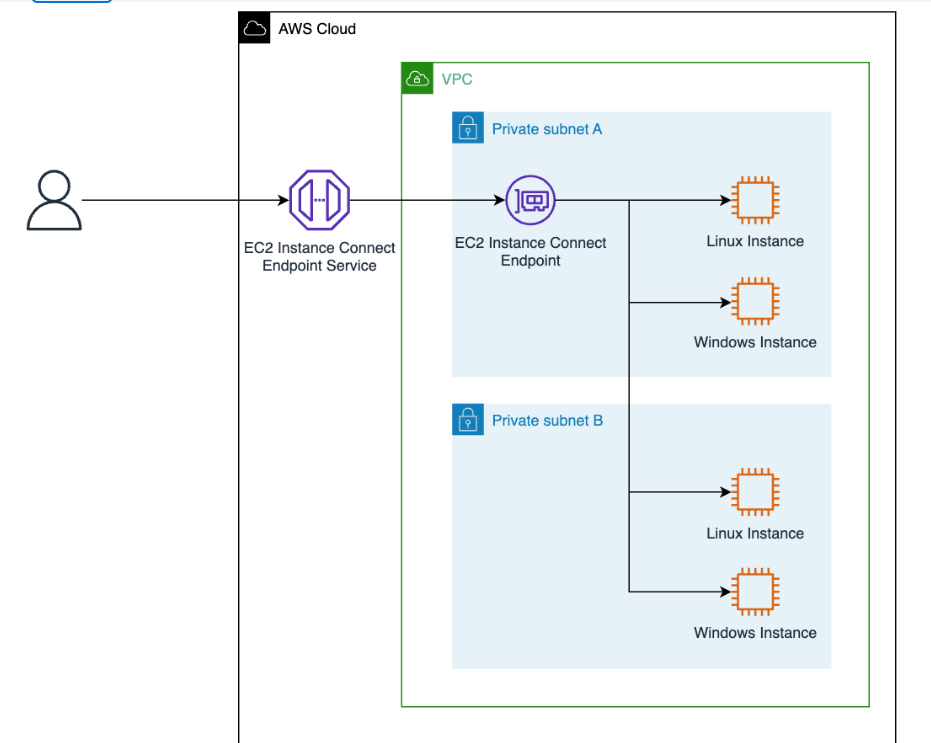
**EC2 Instance Connect in Private Subnets using Instance ID**

EC2 Instance Connect feature allows users to establish SSH or RDP connections to EC2 instances without a public IP address. It supports Unix- and Windows-based systems.

Previously customers had to create a jump box or bastion hosts to tunnel SSH/RDP connections to instances with Private IP addresses. Both involved operational overhead as well as cost. EIC endpoints combine IAM based as well as security group rules-based control and also provide an audit of connections.



**How to connect EC2 instances in Private subnet using Instance ID (Not using public IP)?**

1. **Create IAM Policy for IAM User**

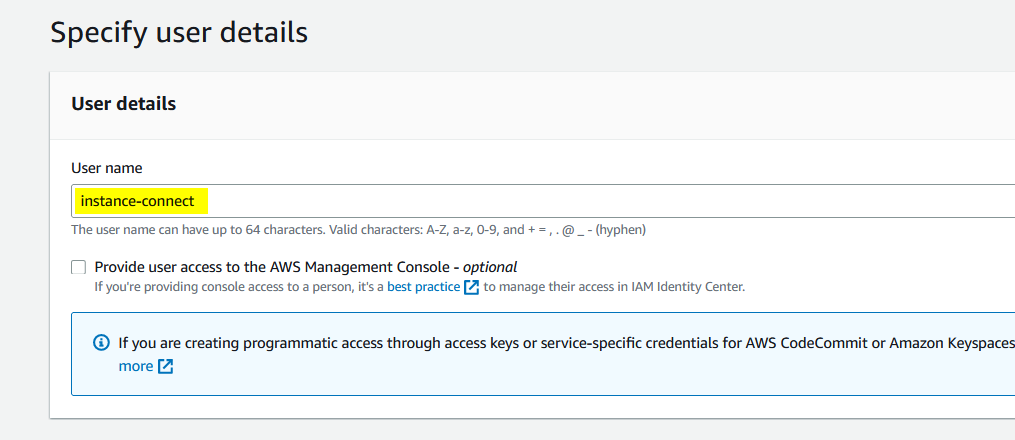
Create Instance connect policy with below link

<https://github.com/kohlidevops/ec2-instance-connect-with-instanceID/blob/main/ec2-instance-connect-policy.json>

Create Instance connect Open tunnel policy with below link

<https://github.com/kohlidevops/ec2-instance-connect-with-instanceID/blob/main/ec2-instance-connect-open-tunnel-policy.json>

1. **Create IAM User with access key and secret key and attach this two policy**



Attach 2 policy to this IAM user

A screenshot of a computer

Description automatically generated with medium confidence

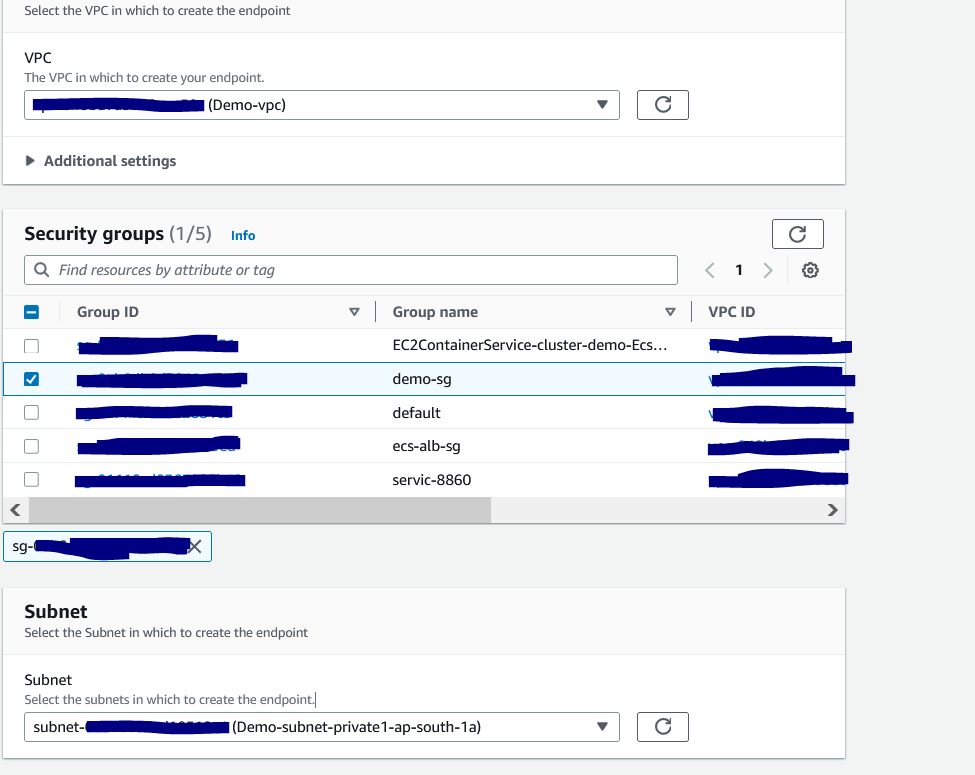
1. **Create Endpoint with EC2 Instance Connect Endpoint**

Navigate to VPC – Select – Endpoint - Create Endpoint

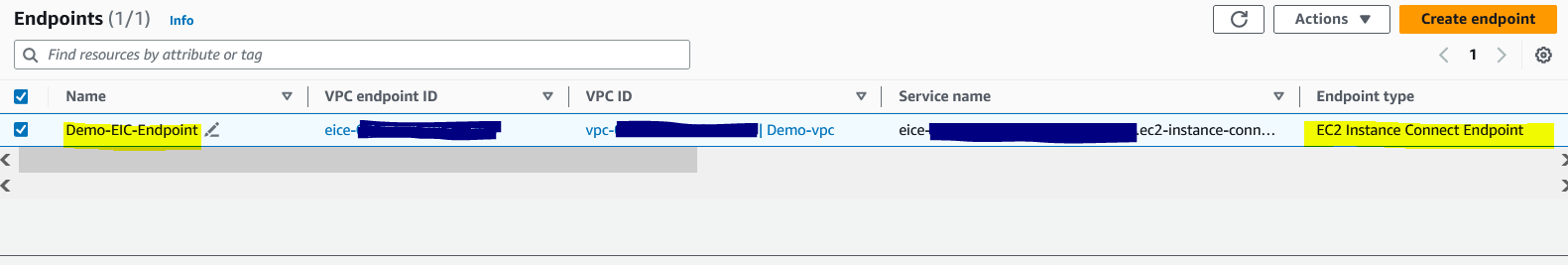
A screenshot of a computer screen

Description automatically generated with medium confidence

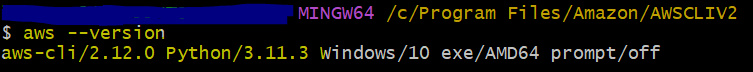
Choose your VPC, Private subnets (where EC2 instances were launched) and Security group



Tags are optional and create a Endpoint



1. **Update your AWS CLI in local system**



//CLI version should be 2.12.0

1. **Configure AWS in local system**

$aws configure

//Provide access-key, secret-key and region

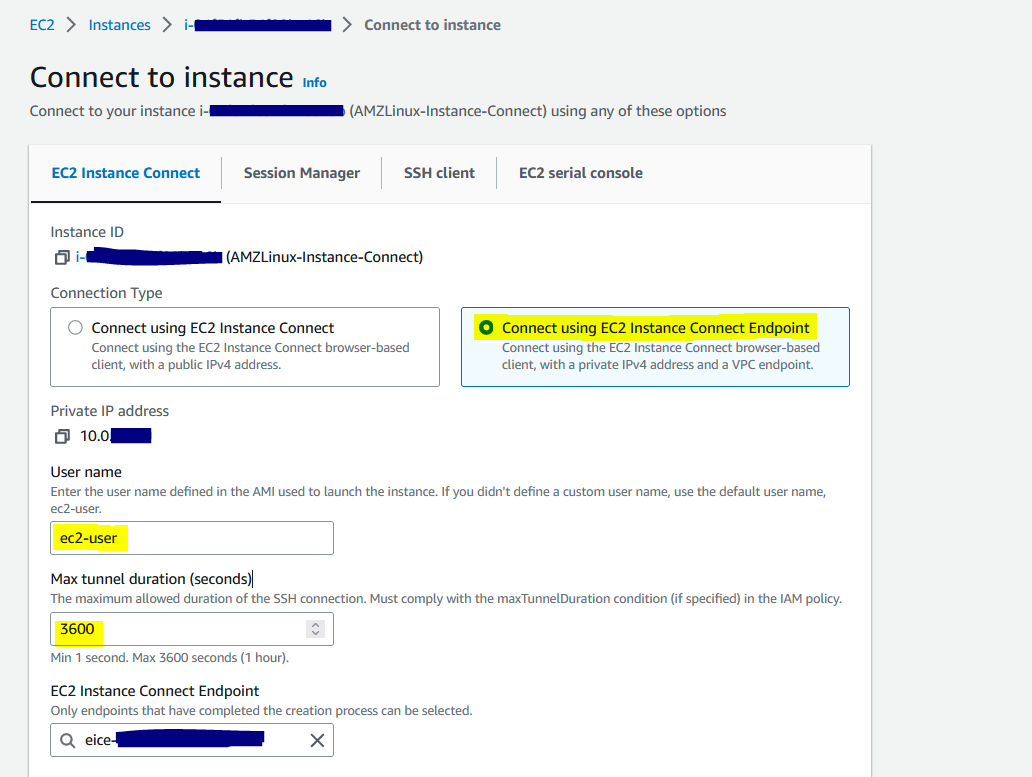
1. **Launch both Windows & Amazon Linux EC2 instance with same VPC**

// Make sure, you select the same subnet for EC2 instance (that you selected to create the endpoint).

A screenshot of a computer

Description automatically generated with medium confidence

// Once the instance has been launched, select and Connect. A new option “Connect using EC2 Instance Connect Endpoint” will show up.



//Alternatively, you can launch using aws-cli in local system

//Here we go, I can able to connect SSH with instance ID

$aws ec2-instance-connect ssh –instance-id <instanceID>

A picture containing text, screenshot, font

Description automatically generated

//Now connect the windows EC2 instance using instance ID

$aws ec2-instance-connect open-tunnel --instance-id <instanceID> --remote-port 3389 --local-port 5555  
A picture containing text, screenshot, software, operating system

Description automatically generated

Its connecting

A screenshot of a computer

Description automatically generated with medium confidence

**Note:**

EIC Endpoint provides a secure solution to connect to your instances via SSH or RDP in private subnets without IGWs, public IPs, agents, and bastion hosts. By configuring an EIC Endpoint for your VPC, you can securely connect using your existing client tools or the Console/AWS CLI.

However, EC2 instance will loose internet connectivity if you are using public subnet.

This features is completely used for Private subnets which should have NATGateway for internet connectivity.

**Refer:**

<https://aws.amazon.com/blogs/compute/secure-connectivity-from-public-to-private-introducing-ec2-instance-connect-endpoint-june-13-2023/>