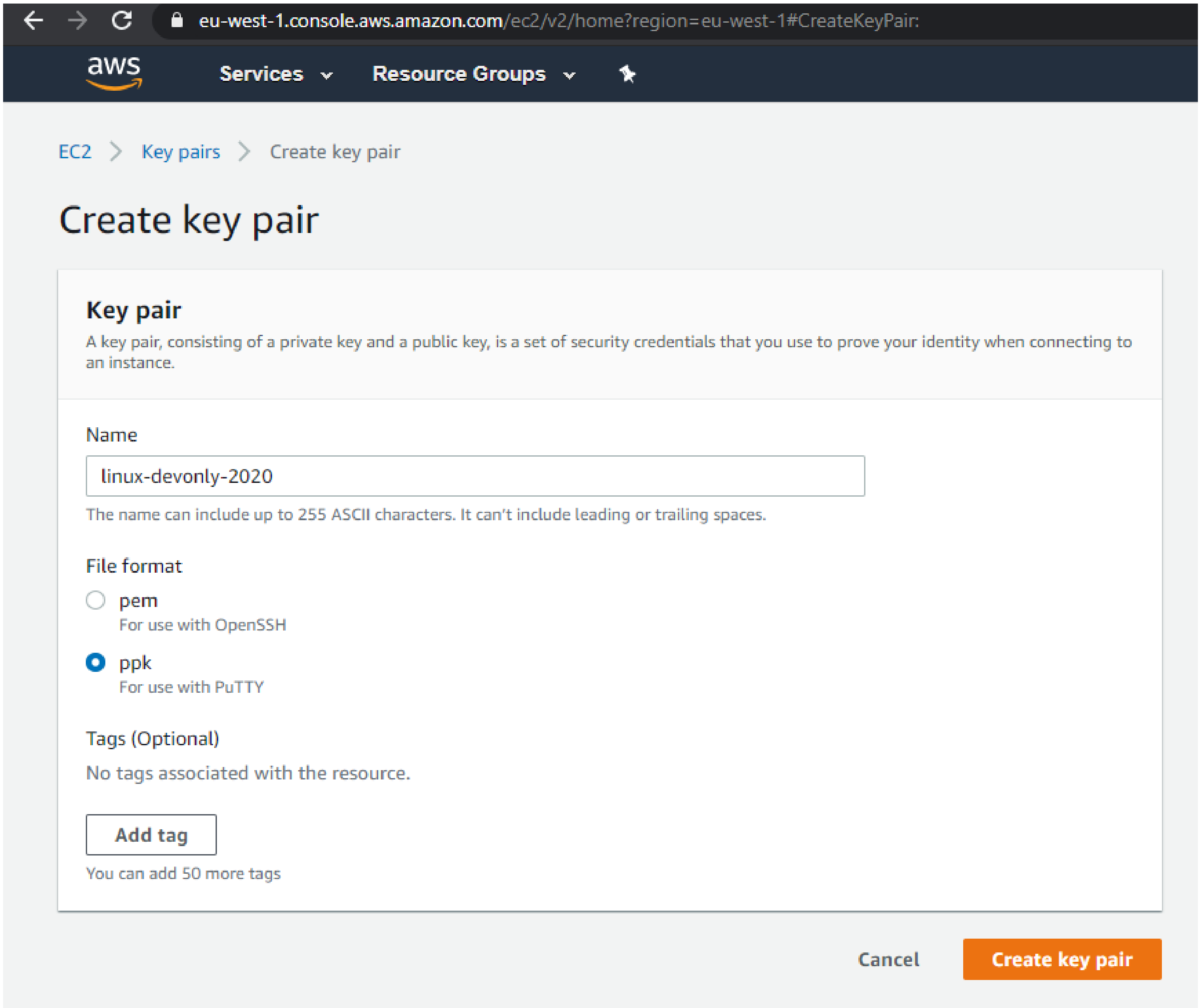
PPK access control with EC2 Linux

Overview

The following article covers the steps required to set ppk access to an EC2 Linux server instance

Steps

1. Create a new AWS key pair under EC2 - Key pairs - Create key pair



eu-west-1.console.aws.amazon.com/ec2/v2/home?region=eu-west-1#CreateKeyPair:

EC2 > Key pairs > Create key pair

Create key pair

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

linux-devonly-2020

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

File format

○ pem
For use with OpenSSH

● ppk
For use with PuTTY

Tags (Optional)

No tags associated with the resource.

You can add 50 more tags

2. Download the newly created ppk file

3. In a notepad file, construct the following syntax. <ssh-rsa> <public key as visible in ppk file> <key label>

ssh-rsa AAAAEj6BSLtoMrsM5 linux-devonly-2020

4. Add the above syntax at the following location as a separate line entry for the authorized_keys file located in **/home/ec2-user/.ssh/authorized_keys** and save/replace the file

5. Connect to the EC2 linux instance using the newly created ppk file to confirm the connection works

ⓘ

Related articles

- Magento site Go live checklist
- Update AWS Launch Configuration and Autoscale Group for Autoscaling
- SQL query to return TOP 400 Expensive queries ran in the last 24 hours
- PPK access control with EC2 Linux