Connecting to a Linux or Unix instance in Amazon EC2 created from an Amazon Lightsail snapshot

Last updated: November 28, 2018

After a Linux or Unix instance is created in Amazon Elastic Compute Cloud (Amazon EC2) from an Amazon Lightsail snapshot, you can connect to the instance via SSH similar to how you connected to the source Lightsail instance. To authenticate to your instance, use either the default Lightsail key pair for the source instance's AWS Region, or your own key pair. This guide shows you how to connect to your Linux or Unix instance in EC2 using PuTTY.

Note
For more information about connecting to a Windows Server instance, see Connecting to a Windows Server instance in Amazon EC2 created from an Amazon Lightsail snapshot.

Contents

Get the key for your instance

Get the correct key required to connect to your new Amazon EC2 instance. The key that you need depends on how you connected to the source Lightsail instance. You may have connected to the source Lightsail instance using one of the following methods:

- **Using the default Lightsail key pair for the source instance's Region** — Download the default private key from the **SSH keys** tab on the Lightsail account page. For more information about the default Lightsail keys, see SSH and connecting to your Lightsail instance. **Note**
After you connect to your EC2 instance, we recommend removing the default Lightsail key from the instance and replacing it with your own key pair. For more information, see Securing your Linux or Unix instance in Amazon EC2 created from an Amazon Lightsail snapshot.
- **Using your own key pair** — Locate your private key and use it to connect to your Amazon EC2 instance. Lightsail does not store your private key when you use your own key pair. If you've lost your private key, you cannot connect to your Amazon EC2 instance.

Get the public DNS address for your instance

Get the public DNS address for your Amazon EC2 instance, so that you can use it when configuring an SSH client, such as PuTTY, to connect to your instance.

To get the public DNS address for your instance

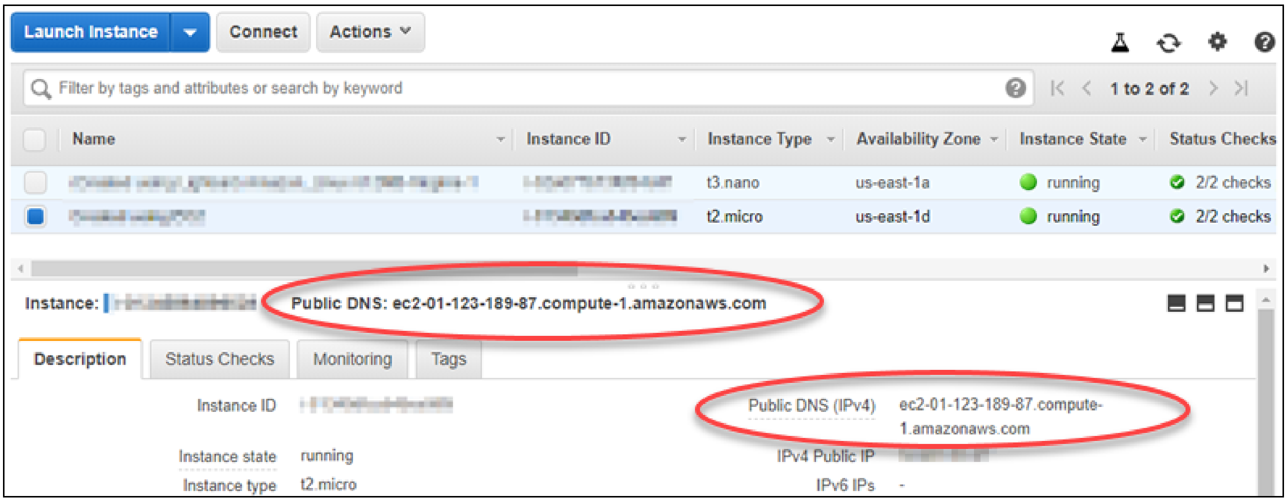
1. Sign in to the Amazon EC2 console.

2. Choose **Instances** from the left navigation pane.

3. Choose the running Linux or Unix instance that you want to connect to.

4. In the lower pane, locate the **Public DNS** address for your instance.

   This is the address that you will use when configuring an SSH client to connect to your instance. Continue to the Download and install PuTTY section of this guide to learn how to download and install the PuTTY SSH client.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
[redacted]	[redacted]	t3.nano	us-east-1a	● running	✓ 2/2 checks
[redacted]	[redacted]	t2.micro	us-east-1d	● running	✓ 2/2 checks

Instance: [redacted] Public DNS: ec2-01-123-189-87.compute-1.amazonaws.com

Instance ID [redacted]

Instance state running

Instance type t2.micro

Public DNS (IPv4) ec2-01-123-189-87.compute-1.amazonaws.com

IPv4 Public IP [redacted]

IPv6 IPs -

Download and install PuTTY

PuTTY is a free SSH client for Windows. For more information about PuTTY, see PuTTY: a free SSH and Telnet client. This website also describes the restrictions in countries where encryption isn't allowed. If you already have PuTTY, you can skip to the following *Configure the key with PuTTYgen* section of this guide.

Download the PuTTY installer or executable file. We recommend using the latest version. However, for information about which download to choose, see the PuTTY documentation.

Continue to the Configure the key with PuTTYgen section of this guide to configure the key with PuTTYgen.

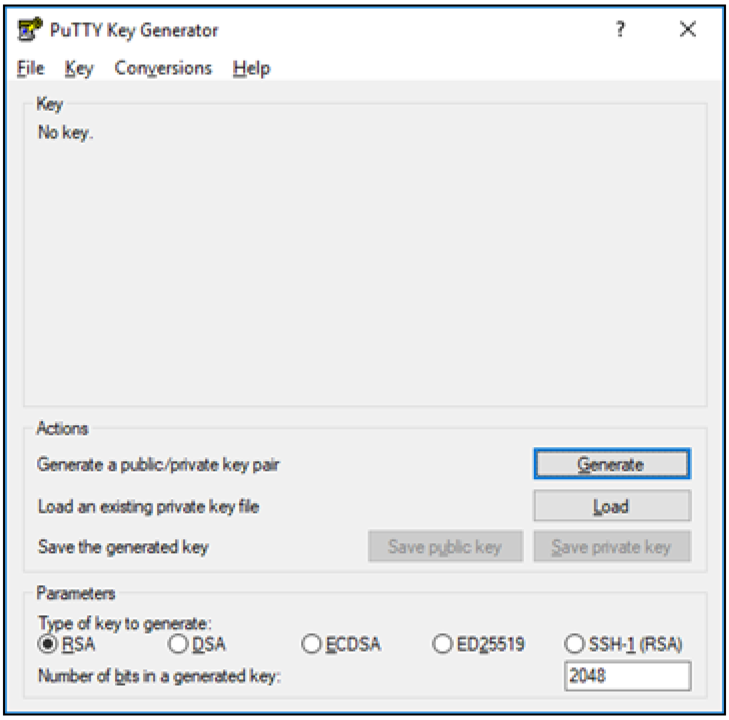
Configure the key with PuTTYgen

PuTTYgen generates pairs of public and private keys to be used with PuTTY. This step is required to use the key file type (.PPK) that PuTTY accepts.

To configure the key with PuTTYgen

1. Start PuTTYgen.

   For example, choose the **Windows Start** menu, choose **All Programs**, choose **PuTTY**, and choose **PuTTYgen**.



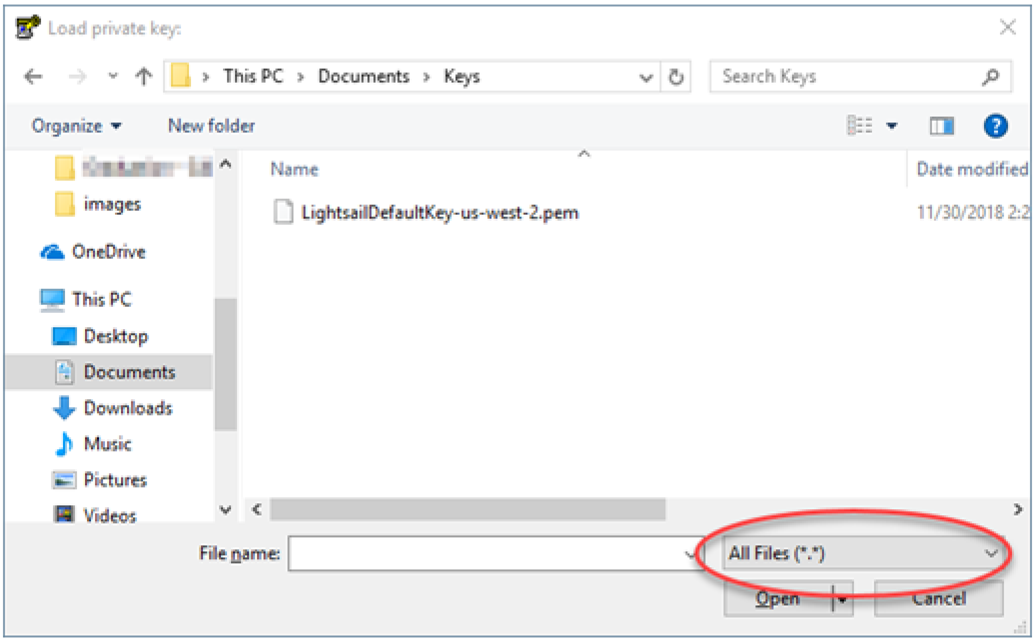
No key.

● RSA

2048

2. Choose **Load**.

   By default, PuTTYgen displays only files with the .PPK extension. To locate your .PEM file, select the option to display files of all types.

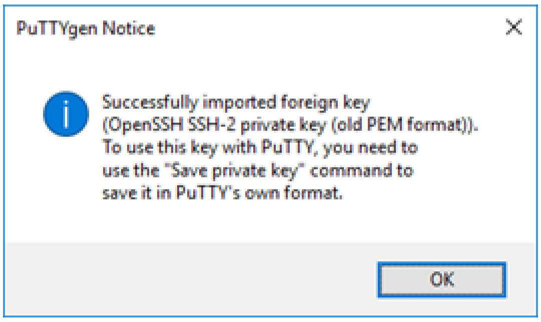


LightsailDefaultKey-us-west-2.pem 11/30/2018 2:2

All Files (*.*)

3. Choose the default Lightsail key file (.PEM) that you downloaded earlier in this guide, and then choose **Open**.

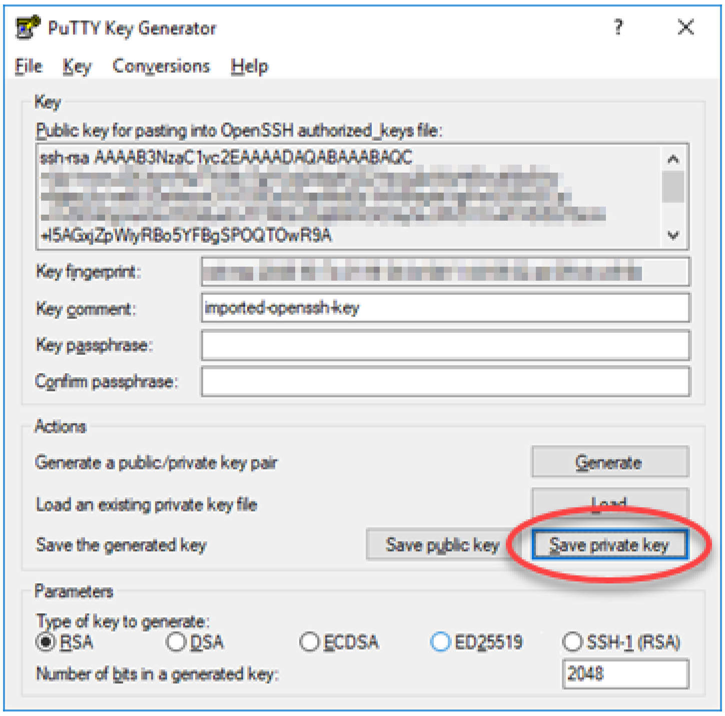
4. After PuTTYgen confirms that you successfully imported the key, choose **OK**.



Successfully imported foreign key (OpenSSH SSH-2 private key (old PEM format)). To use this key with PuTTY, you need to use the "Save private key" command to save it in PuTTY's own format.

5. Choose **Save private key**, and then confirm that you don't want to save it with a passphrase.

   If you create a passphrase as an extra measure of security, you must enter it every time you connect to your instance using PuTTY.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC
[redacted]
+I5AGxjZpWlyRBo5YFBgSPOQTOwR9A
```

Key fingerprint: [redacted]

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

6. Specify a name and a location to save your private key, and then choose **Save**.

   PuTTYgen saves your new key file as a .PPK file type.

7. Close PuTTYgen.

   Continue to the Configure PuTTY to connect to your instance section of this guide to use the new .PPK file that you generated to configure PuTTY and connect to your Linux or Unix instance in Amazon EC2.

Configure PuTTY to connect to your instance

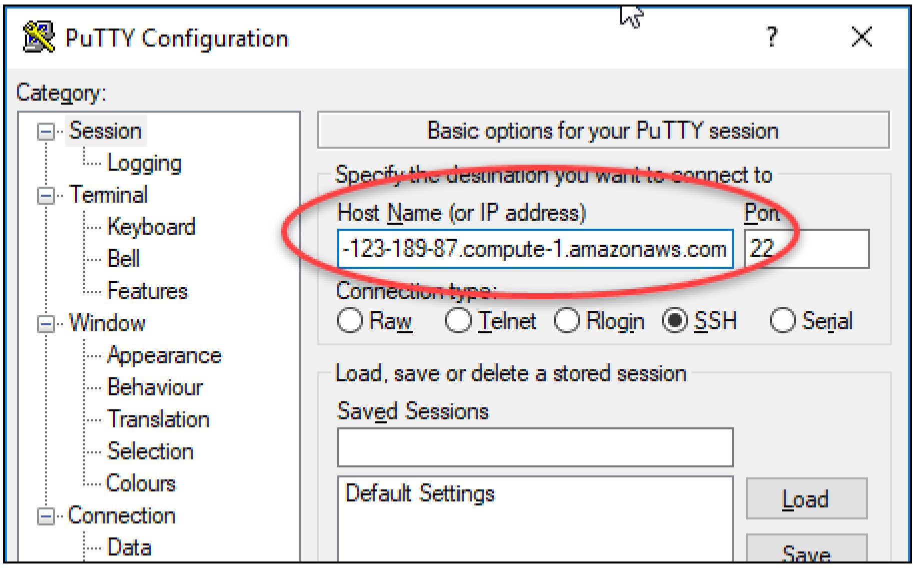
Configure PuTTY, now that you have all of the requirements to connect to your Linux or Unix instance using SSH.

To configure PuTTY to connect to your Linux or Unix instance

1. Open PuTTY.

For example, choose the **Windows Start** menu, choose **All Programs**, choose **PuTTY**, and choose **PuTTY**.

2. In the **Host Name** text box, enter the public DNS address for your instance that you obtained from the Amazon EC2 console earlier in this guide.



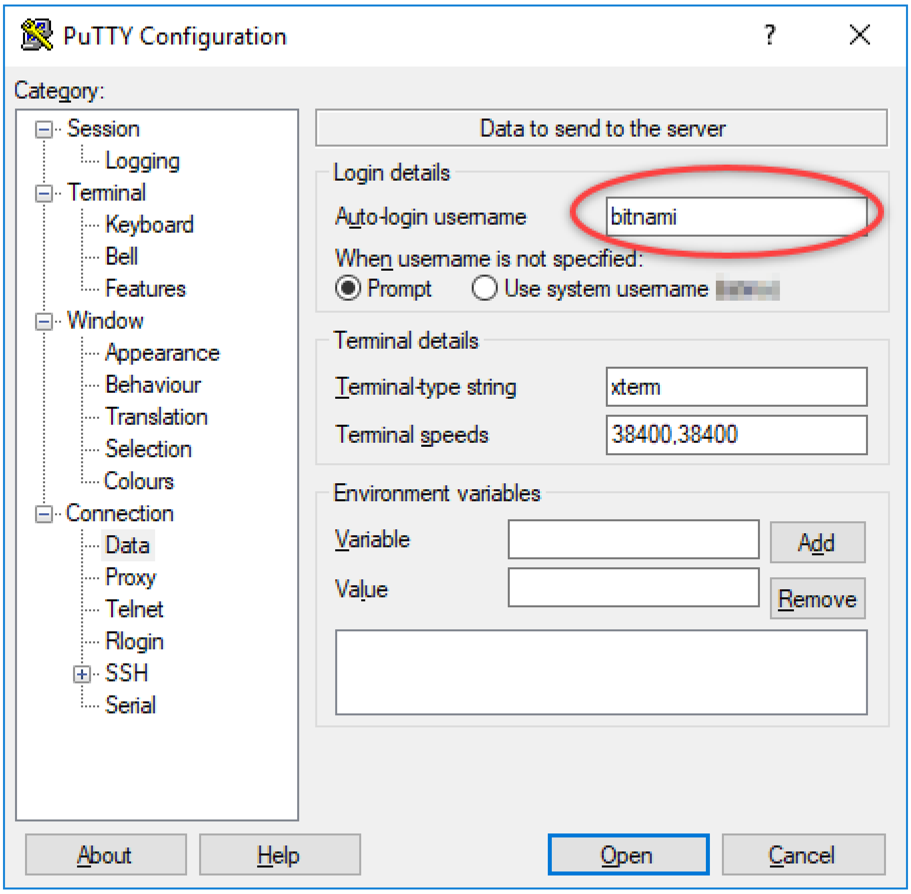
Host Name (or IP address): -123-189-87.compute-1.amazonaws.com

Port: 22

● SSH

3. Under the **Connection** section in the left navigation pane, choose **Data**.

4. In the **Auto-login username** text box, enter a user name to use when logging in to the instance.



Auto-login username: bitnami

● Prompt ○ Use system username [redacted]

Terminal-type string: xterm

Terminal speeds: 38400,38400

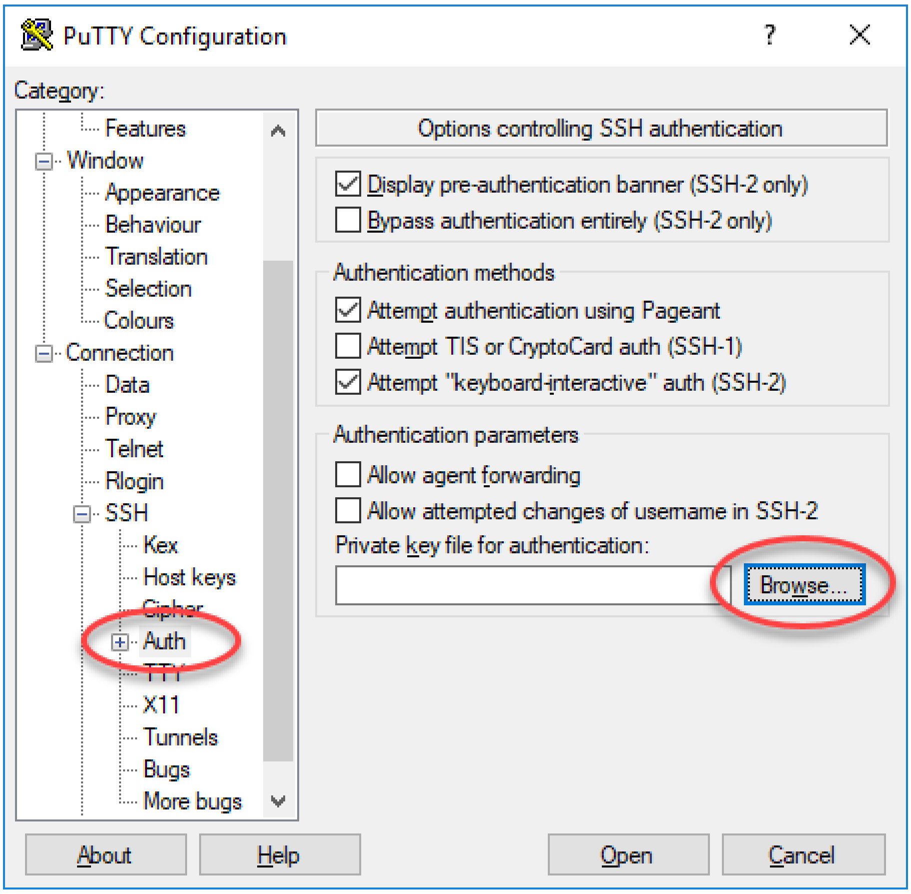
Enter one of the following default user names depending on the blueprint of the source Lightsail instance:

- Amazon Linux, openSUSE, and FreeBSD instances: `ec2-user`
- CentOS instances: `centos`

- Debian instances: `admin`
- Ubuntu instances: `ubuntu`
- "Powered by Bitnami" instances: `bitnami`
- Plesk instances: `ubuntu`

5. Under the **Connection** section in the left navigation pane, expand **SSH**, and then choose **Auth**.

6. Choose **Browse** to navigate to the .PPK file that you created in the previous section of this guide, and then choose **Open**.



Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
☐ Bypass authentication entirely (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

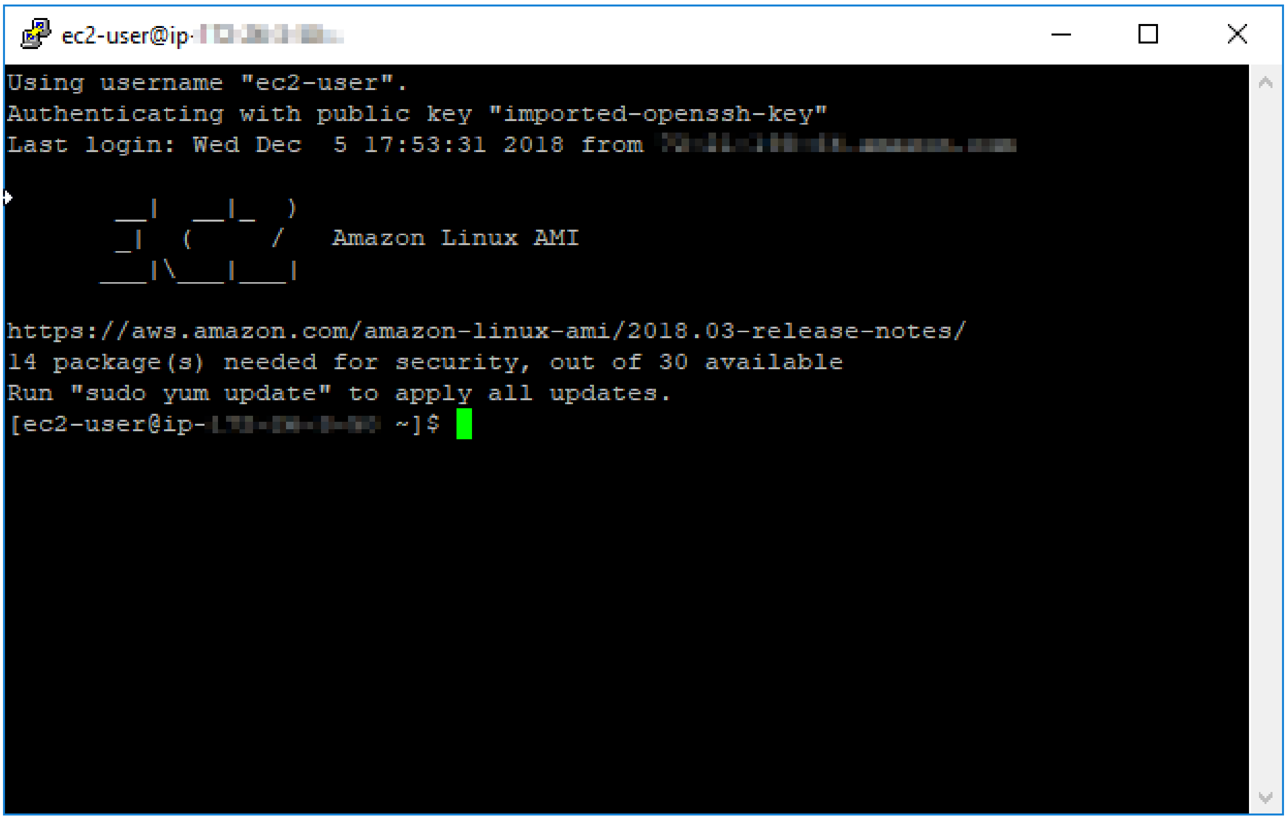
Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

7. Choose **Open** to connect to your instance, and then choose **Yes** to trust this connection in the future.

You should see a screen similar to the following if you've successfully connected to your instance:



```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Wed Dec  5 17:53:31 2018 from [redacted]

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
14 package(s) needed for security, out of 30 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-[redacted] ~]$ 
```

Next steps

Your new Linux or Unix instance in Amazon EC2 contains residual keys from the Lightsail service, if you use Amazon EC2 to create new instances from your exported snapshots. We recommend removing these keys to enhance security for your new Amazon EC2 instance. For more information, see Securing your Linux or Unix instance in Amazon EC2 created from a Lightsail snapshot.