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

Last updated: November 28, 2018

Amazon Lightsail, and Amazon Elastic Compute Cloud (Amazon EC2), use public–key cryptography to encrypt and decrypt login information. Public–key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair.

When you export a Linux or Unix Lightsail instance to EC2, the new EC2 instance will contain residual keys from the Lightsail service. As a security best practice, you should remove unused keys from your instance.

To improve the security of a Linux or Unix instance in EC2 that was created from a Lightsail snapshot, we recommend that you perform the following actions after creating the instance:

- Remove and replace the Lightsail default key if you used it to connect to the source instance in Lightsail. The Lightsail default key is not present in your Amazon EC2 instance if you used your own key to connect to your instance, or you created an key for your instance in the Lightsail console.
- Remove the Lightsail system key, also known as the `lightsail_instance_ca.pub` key. This key on Linux and Unix instances enables the Lightsail browser-based SSH client to connect. The `lightsail_instance_ca.pub` key is automatically removed when an EC2 instance is created using the **Create an Amazon EC2 instance** page in the Lightsail console or the Lightsail API.
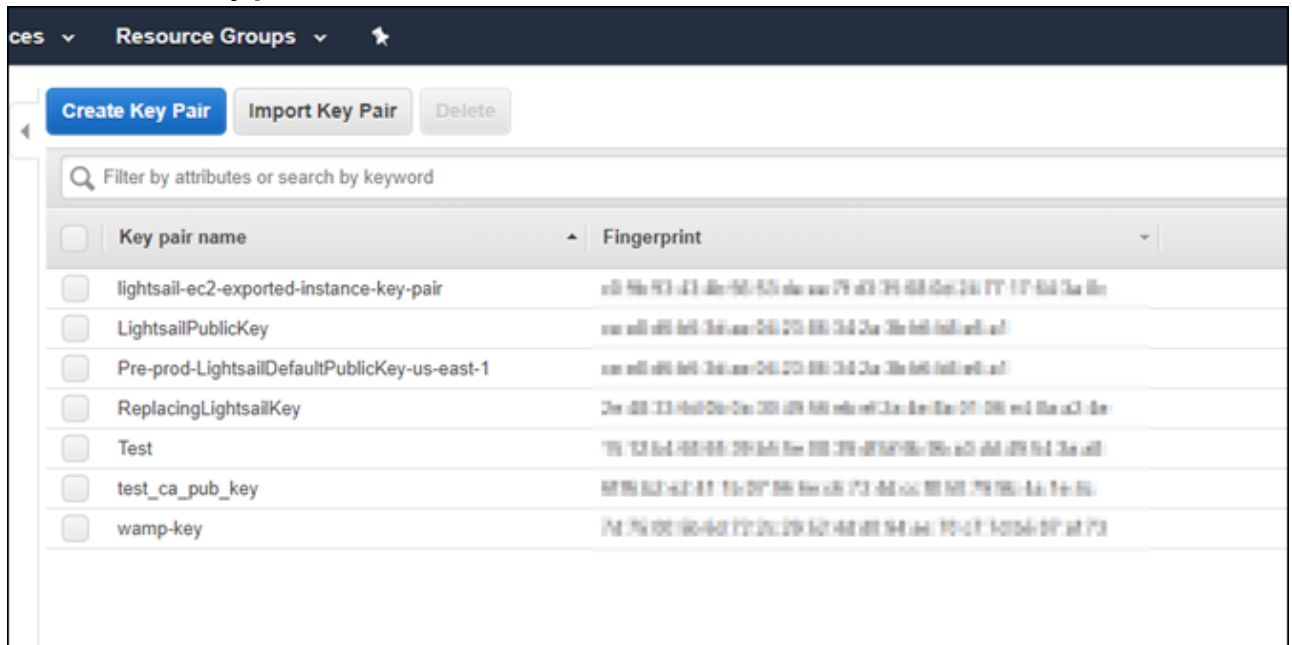
Contents

Create a private key using Amazon EC2

Use the Amazon EC2 console to create a new key pair that you can use to replace the Lightsail default key pair.

To create a private key using Amazon EC2

1. Sign in to the Amazon EC2 console.

2. From the left navigation pane, choose **Key Pairs**.

3. Choose **Create key pair**.

4. Enter a name for the key into the **Key pair name** text box, then choose **Create**.

   The new private key is automatically downloaded. Make note of where the private key is saved. You need it in the following *Create the public key using PuTTYgen* section of this guide to create a public key.
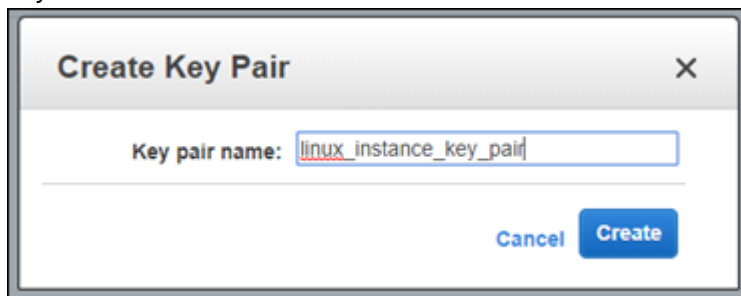
Create the public key using PuTTYgen

PuTTYgen is a tool that is included with PuTTY. Use PuTTYgen to generate the public key text that you add to your instance later in this guide.
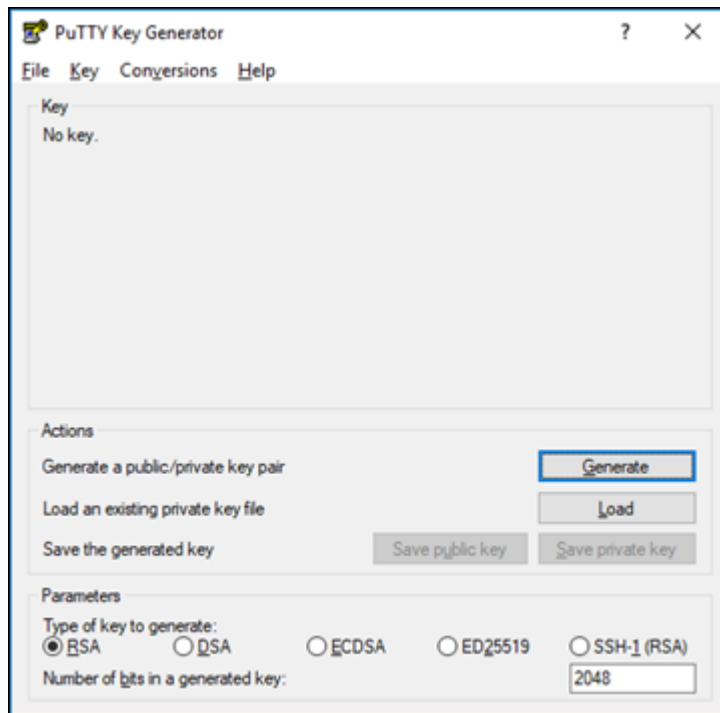
Note

For more information about how to configure PuTTY to connect to your Linux or Unix instance, see Connecting to a Linux or Unix instance in Amazon EC2 created from an Amazon Lightsail snapshot.
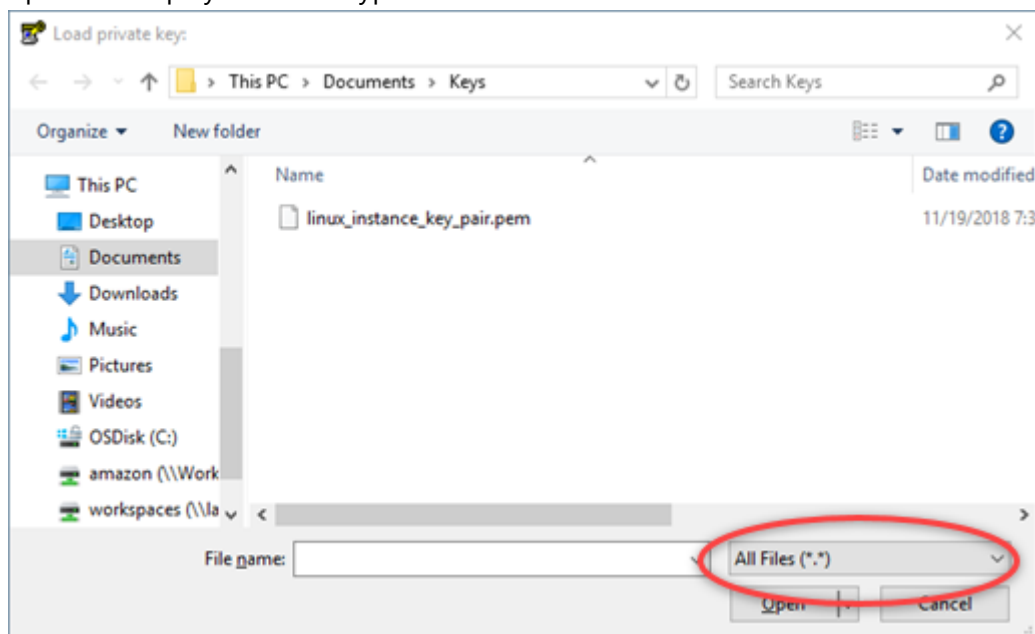
To create the public key using PuTTYgen

1. Start PuTTYgen.

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

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.

3. Navigate to the location of your private key that was created earlier in this guide. Choose the private key, and then choose **Open**.

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

5. Highlight the contents of the **Public key** text box and copy it to your clipboard by pressing **Ctrl+C** if you're using Windows, or **Cmd+C** if you're using macOS.

   Open a text editor, such as Notepad or TextEdit, and paste the public key text into it by pressing **Ctrl+V** if you're using Windows, or **Cmd+V** if you're using macOS. Save the file with your public key text; you

will need it later in this guide.
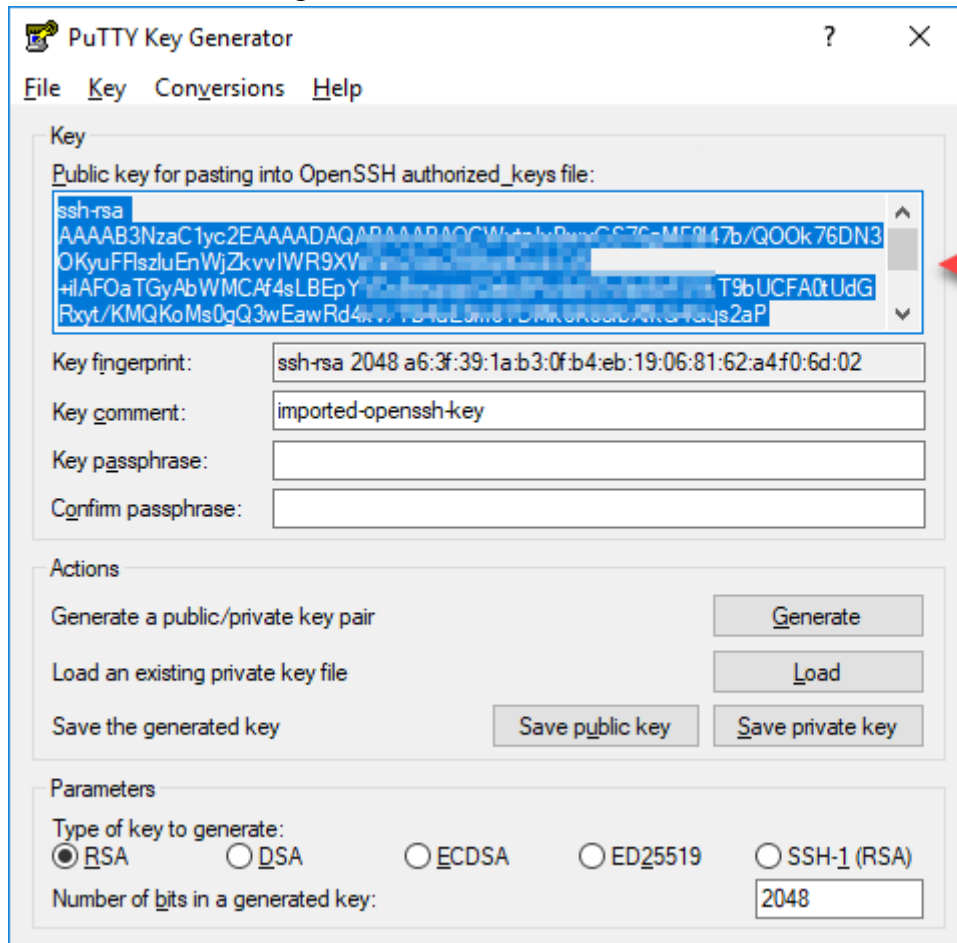
6. Continue to the Connect to your Linux or Unix instance in Amazon EC2 section of this guide to connect to your EC2 instance and add the public key.

Connect to your Linux or Unix instance in Amazon EC2

Connect to your Linux or Unix instance in Amazon EC2 using SSH to remove the Lightsail default key and system key. For more information, see Connecting to a Linux or Unix instance in Amazon EC2 created from an Amazon Lightsail snapshot.

Continue to the Add the public key to your instance and test the connection section of this guide after you're connected to your instance in Amazon EC2.

Add the public key to your instance and test the connection

Public key content is saved in the `~/.ssh/authorized_keys` file on Linux and Unix instances. Edit the file to remove and replace the Lightsail default key from your Linux or Unix instance in Amazon EC2.

To add the public key to your instance and test the connection

1. After you establish an SSH connection to your instance, enter the following command to edit the `authorized_keys` file using the Vim text editor.

```
sudo vim ~/.ssh/authorized_keys
```

Note

These steps use Vim for demonstration purposes. However, you can use any text editor for these steps.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCqPFGPJSLOaAMzjPfUv2fpgkoHFohXJpybmXVisPuC
v6iGYfmb8flA89Eel4bKrlX                                                    L2wGMn
GyGFjY/wONNp3/8wNfeReiZ                                                    RwC/uI
+tY/T3dxQvMI0TilPv5mhUL                                                   6Rvv8a
cbpEv3ISF9vdmsUs8kUlayF                                       LightsailDefaultKey
Pair
~
~
~
```

1. Press the `I` key to enter the insert mode in the Vim editor.

2. Enter an extra line after the Lightsail default key.

3. Copy and paste the public key text that you saved earlier in this guide.

   The result should look like the following:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCqPFGPJSLOaAMzjPfUv2fpgkoHFohXJpybmXVisPuC     Lightsail default key


cbpEv3ISF9vdmsUs8kUlayFlKuFIIc+TVLjKlK+PYkxVH+0qPZevu2gd9R2f LightsailDefaultKey
Pair
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCWvtpIvBwvGS76gMF8l47b/QOOk76DN3OKyuFFlszl     New key


Pymgci5iWdhx1a8aDpgEvClwjsw+P9c7380QNy9PsUkiflYmJEOOOSb9czuR imported-openssh-ke
y
~
~
```

4. Press the `ESC` key, and then enter `:wq` to write, or save, your edits, and quit Vim.

5. Enter the following command to restart the Open SSH server:

   ```
   sudo /etc/init.d/sshd restart
   ```

   You should see a result similar to the following:

```
[ec2-user@ip-172-26-11-173 ~]$ sudo /etc/init.d/sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[ec2-user@ip-172-26-11-173 ~]$ █
```

   Your new public key is now added to your instance. To test the new key pair, disconnect from your instance. Configure PuTTY to use your new private key instead of the Lightsail default key. If you're able to successfully connect to your instance using your new key pair, continue to the Remove the Lightsail default key section of this guide to remove the Lightsail default key.

Remove the Lightsail default key

Remove the Lightsail default key after you've added a new public key to your instance, and successfully connected to it using the new key pair.

To remove the Lightsail default key

1. After you establish an SSH connection to your instance, enter the following command to edit the `authorized_keys file` using the Vim text editor.

   ```
   sudo vim ~/.ssh/authorized_keys
   ```

2. Press the `I` key to enter the insert mode in the Vim editor.

3. Delete the line that ends with `LightsailDefaultKeyPair`. This is the Lightsail default key.

4. Press the `ESC` key, and then enter `:wq` to write, or save, your edits, and quit Vim.

5. Enter the following command to restart the Open SSH server:

   ```
   sudo /etc/init.d/sshd restart
   ```

   You should see a result similar to the following:

   The Lightsail default key is now removed from your instance. Your instance will now refuse connections that use the Lightsail default key. Continue to the Remove the Lightsail system key section of this guide to remove the Lightsail system key.

Remove the Lightsail system key

The Lightsail system key, also known as the `lightsail_instance_ca.pub` key, on Linux and Unix instances enables the Lightsail browser-based SSH client to connect. Perform the following steps to remove the `lightsail_instance_ca.pub` key from your Linux or Unix instance in Amazon EC2, and edit the `/etc/ssh/sshd_config` file. The `/etc/ssh/sshd_config` file defines parameters for SSH connections to your instance.

To remove the Lightsail system key

1. In an SSH terminal window connected to your instance, enter the following command to remove the `lightsail_instance_ca.pub` key:

```
sudo rm -r /etc/ssh/lightsail_instance_ca.pub
```

2. Enter the following command to edit the `sshd_config` file using the Vim text editor.

```
sudo vim /etc/ssh/sshd_config
```

3. Press the `I` key to enter the insert mode in the Vim editor.

4. Delete the following text from the file, if it's present:

```
TrustedUserCAKeys /etc/ssh/lightsail_instance_ca.pub
```

5. Press the `ESC` key, and then enter `:wq` to write, or save, your edits, and quit Vim.

6. Enter the following command to restart the Open SSH server:

```
sudo /etc/init.d/sshd restart
```

You should see a result similar to the following:

```
[ec2-user@ip-172-26-11-173 ~]$ sudo /etc/init.d/sshd restart
Stopping sshd:                                              [  OK  ]
Starting sshd:                                              [  OK  ]
[ec2-user@ip-172-26-11-173 ~]$ 
```

The `lightsail_instance_ca.pub` key is now removed from your instance. The associated `sshd_config` file is updated to exclude that key.