Connecting RAKwireless Commercial Gateways to the Cloud

AWS + ChirpStack

Version V1.1 | April 2020

www.RAKwireless.com

Visit our website for more document.

Table of Contents

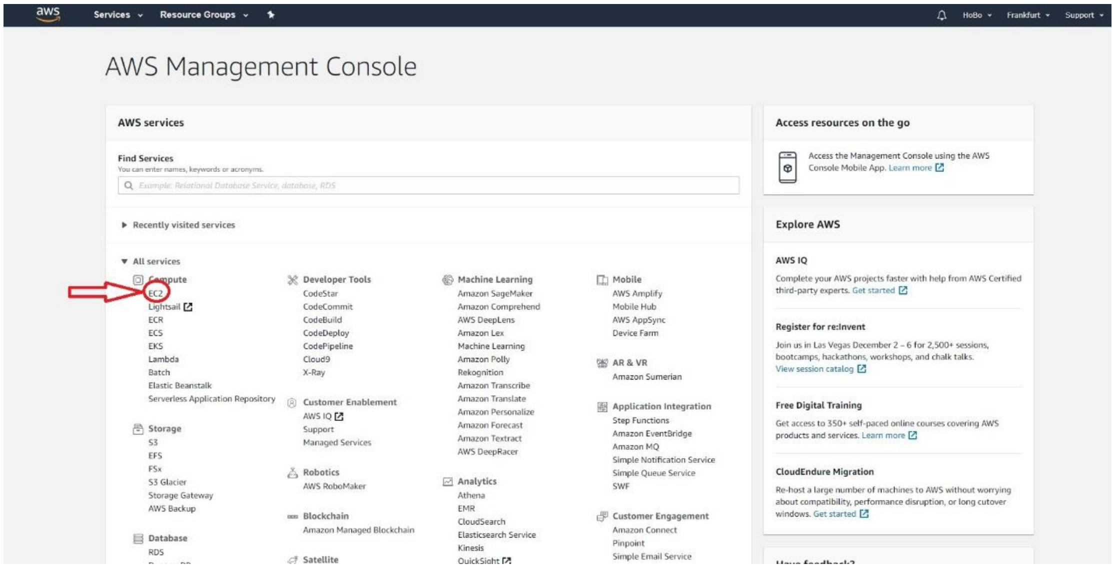
1 Amazon Web Services

1.1 Creating an account

Amazon offers a free cloud service (aws.amazon.com); you only need to make an Amazon account. There is a limit however: 750 hours per month for a period of 12 months. It is to be noted that you need a debit card to verify your identity in order to use the service.

1.2 Selecting an running an instance

After you have logged into your account you need to select what instance you are going to be running. Fort the purpose of this tutorial we are going to be using EC2. Select it in the AWS Management Console.



Access resources on the go

Access the Management Console using the AWS Console Mobile App. Learn more

Explore AWS

AWS IQ

Complete your AWS projects faster with help from AWS Certified third-party experts. Get started

Register for re:Invent

Join us in Las Vegas December 2 – 6 for 2,500+ sessions, bootcamps, hackathons, workshops, and chalk talks. View session catalog

Free Digital Training

Get access to 350+ self-paced online courses covering AWS products and services. Learn more

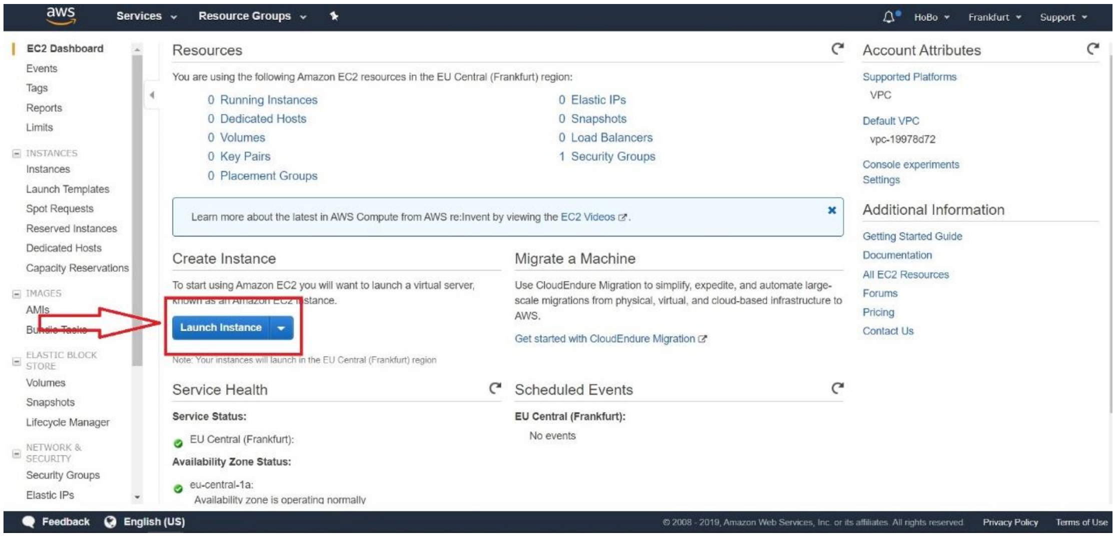
CloudEndure Migration

Re-host a large number of machines to AWS without worrying about compatibility, performance disruption, or long cutover windows. Get started

Figure 1 | AWS Management Console

In the following screen you can see your running instances, key pairs, security groups, etc.

Press the blue “Launch instance” button.



Resources

You are using the following Amazon EC2 resources in the EU Central (Frankfurt) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent by viewing the EC2 Videos.

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the EU Central (Frankfurt) region

Migrate a Machine

Use CloudEndure Migration to simplify, expedite, and automate large-scale migrations from physical, virtual, and cloud-based infrastructure to AWS.

Get started with CloudEndure Migration

Service Health

Service Status:

EU Central (Frankfurt):

Availability Zone Status:

eu-central-1a:
Availability zone is operating normally

Scheduled Events

EU Central (Frankfurt):

No events

Account Attributes

Supported Platforms
VPC

Default VPC
vpc-19978d72

Console experiments
Settings

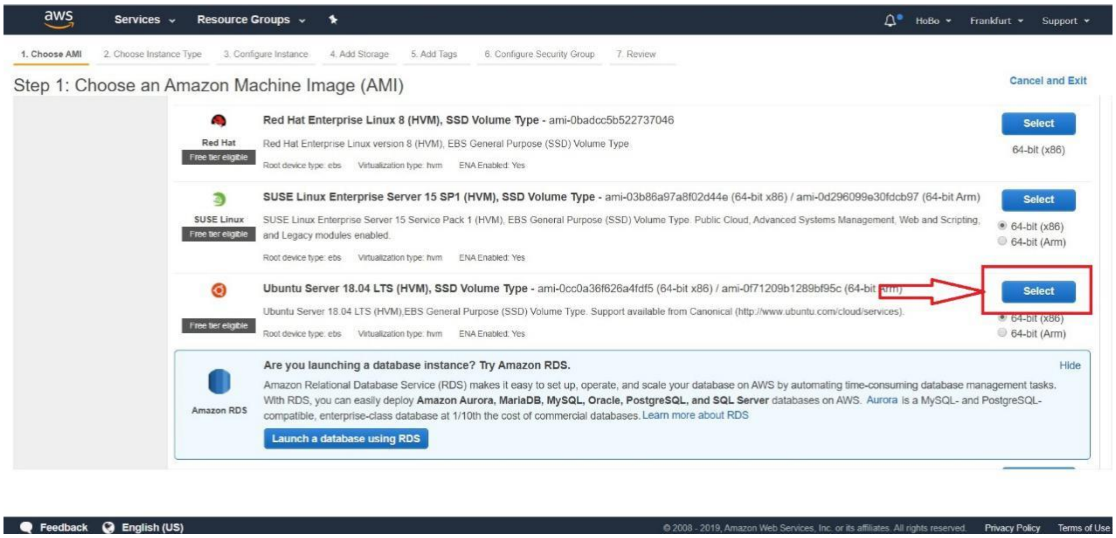
Additional Information

Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Figure 2 | Launching an Instance

The is a ton of choices for the operating system, however we will be using Ubuntu. Scroll down and choose Ubuntu Server 18.04 LTS (latest at the time of this document). Click the “Select” button.



Step 1: Choose an Amazon Machine Image (AMI)

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0badcc5b522737046
Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

SUSE Linux Enterprise Server 15 SP1 (HVM), SSD Volume Type - ami-03b86a97a8f02d44e (64-bit x86) / ami-0d296099e30fdcb97 (64-bit Arm)
SUSE Linux Enterprise Server 15 Service Pack 1 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
● 64-bit (x86)
○ 64-bit (Arm)

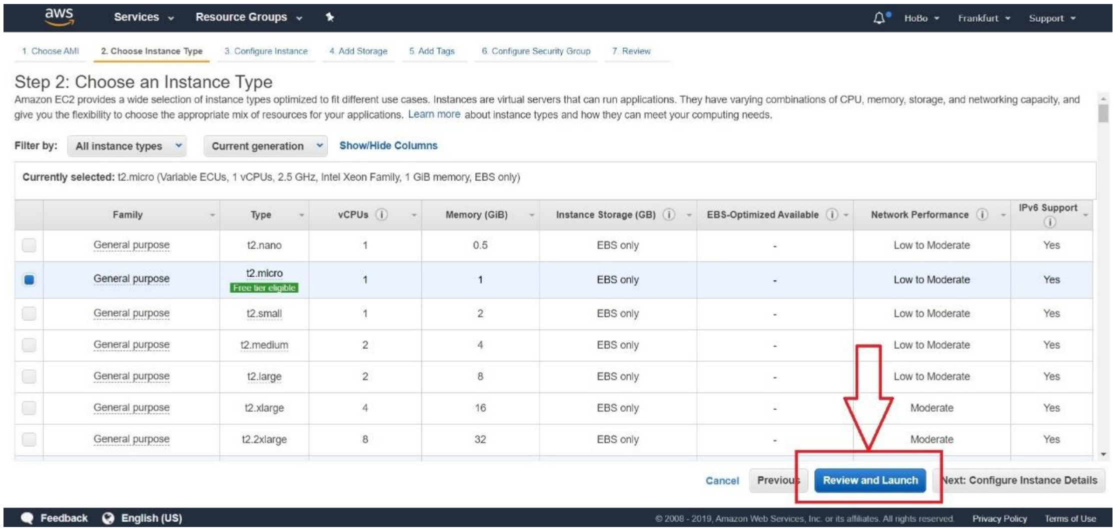
Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0cc0a36f626a4fdf5 (64-bit x86) / ami-0f71209b1289bf95c (64-bit Arm)
Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
● 64-bit (x86)
○ 64-bit (Arm)

Are you launching a database instance? Try Amazon RDS.
Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora, MariaDB, MySQL, Oracle, PostgreSQL, and SQL Server** databases on AWS. Aurora is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. Learn more about RDS

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Figure 3 | Selecting the Operating System

In the next window you can configure your Instance, however we will leave it as it is. Just select the *t2.Micro* for the instance type as in Figure 4 and click “Review and Launch”



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation | Show/Hide Columns

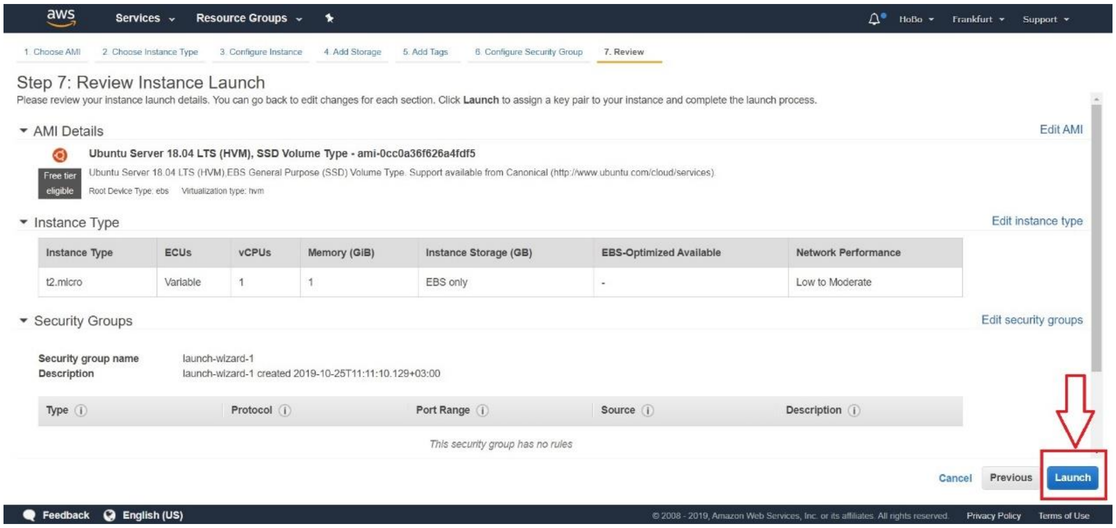
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes

Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Figure 4 | Selecting the Operating System

Confirm your choice and Launch (Figure 5). Security groups will be edited in the next section so you can go ahead and confirm your choice by pressing the “Launch” button (Figure 5).



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details — Edit AMI

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0cc0a36f626a4fdf5

Free tier eligible

Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Root Device Type: ebs Virtualization type: hvm

Instance Type — Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups — Edit security groups

Security group name launch-wizard-1
Description launch-wizard-1 created 2019-10-25T11:11:10.129+03:00

Type	Protocol	Port Range	Source	Description

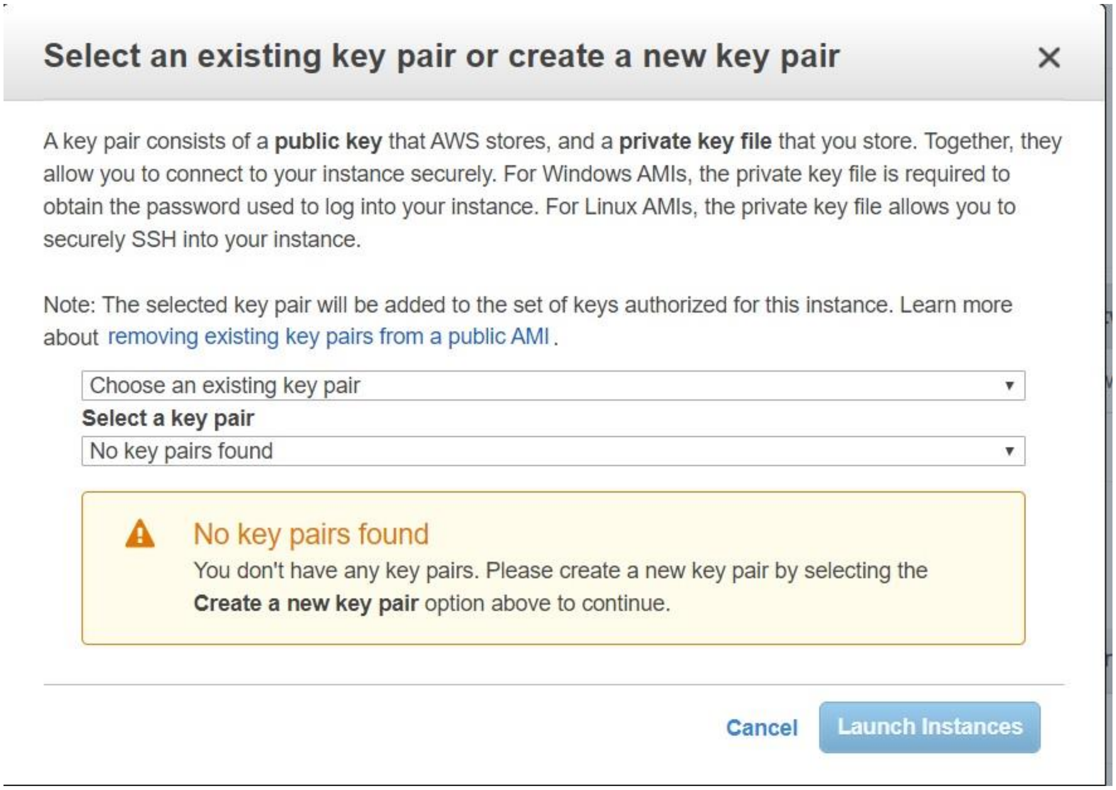
This security group has no rules

Cancel
Previous
Launch
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Figure 5 | Launching the Instance

1.3 Creating Keys and accessing the AWS Instance via SSH

In order to have an SSH session to the Instance we need to create the appropriate access keys. Thus, after Launching you will see the window in Figure 6.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Choose an existing key pair

Select a key pair

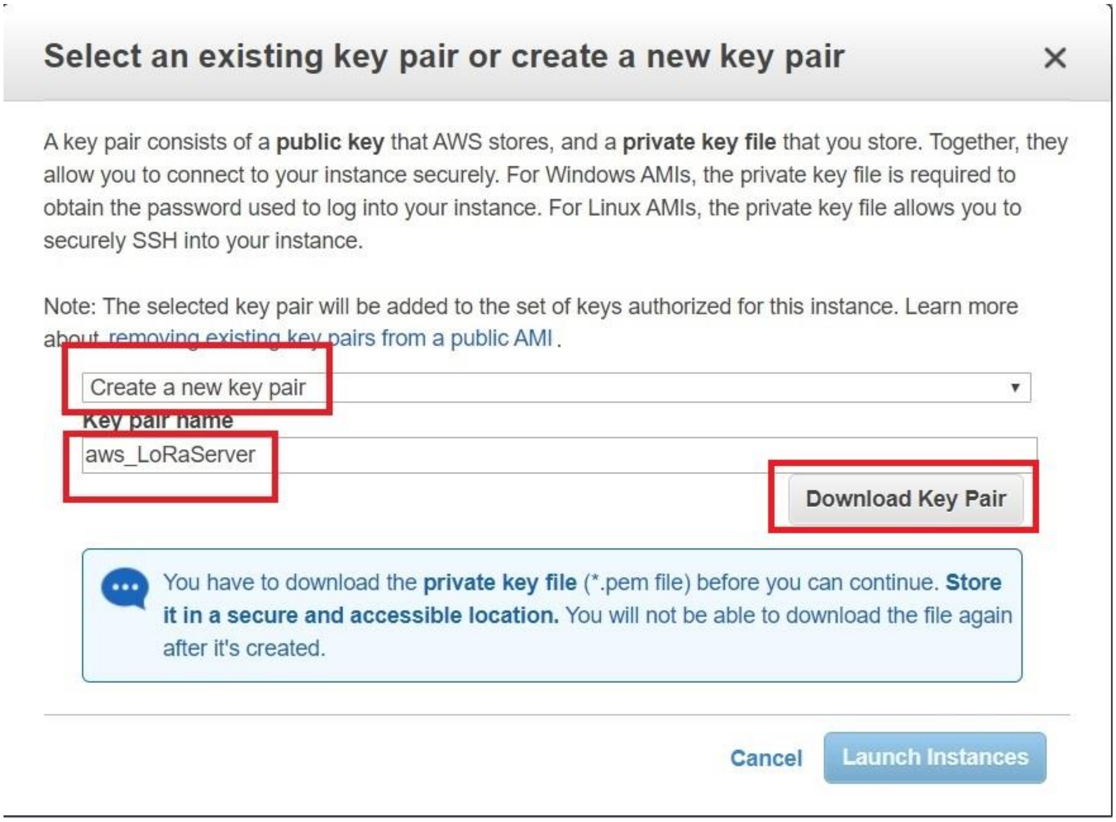
No key pairs found

No key pairs found

You don't have any key pairs. Please create a new key pair by selecting the **Create a new key pair** option above to continue.

Figure 6 | Key pair creation

We will choose to Create a new key pair from the drop-down menu and give it an appropriate name. Finally click the “Download Key Pair” button (Figure 7).



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name

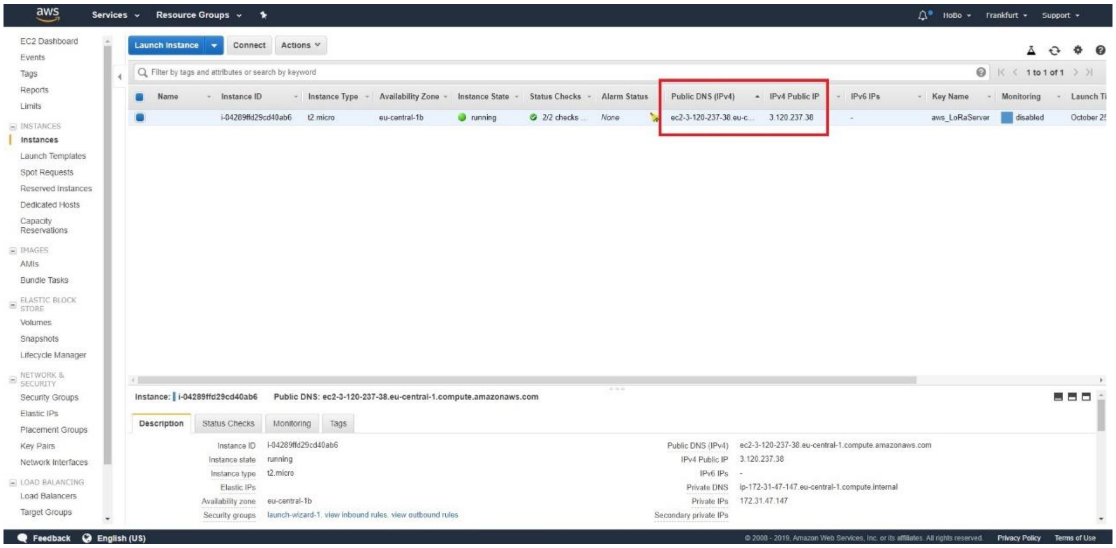
aws_LoRaServer

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Figure 7 | Creating a new key pair

After saving the Keys to a location of your choosing you can Launch the instance via the blue button (Figure 7).

In Figure 8 below you can see the parameters of your instance. Note the fields in the highlighted with the red rectangle. These are you real URL and IP Address for accessing this instance (those are just an example; you will have a different set).



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring	Launch Ti
	i-04289ffd29cd40ab6	t2.micro	eu-central-1b	running	2/2 checks ...	None	ec2-3-120-237-38.eu-c...	3.120.237.38	-	aws_LoRaServer	disabled	October 25

Instance: i-04289ffd29cd40ab6 Public DNS: ec2-3-120-237-38.eu-central-1.compute.amazonaws.com

Description | Status Checks | Monitoring | Tags

Instance ID	i-04289ffd29cd40ab6	Public DNS (IPv4)	ec2-3-120-237-38.eu-central-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	3.120.237.38
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-31-47-147.eu-central-1.compute.internal
Availability zone	eu-central-1b	Private IPs	172.31.47.147
Security groups	launch-wizard-1. view inbound rules. view outbound rules	Secondary private IPs	

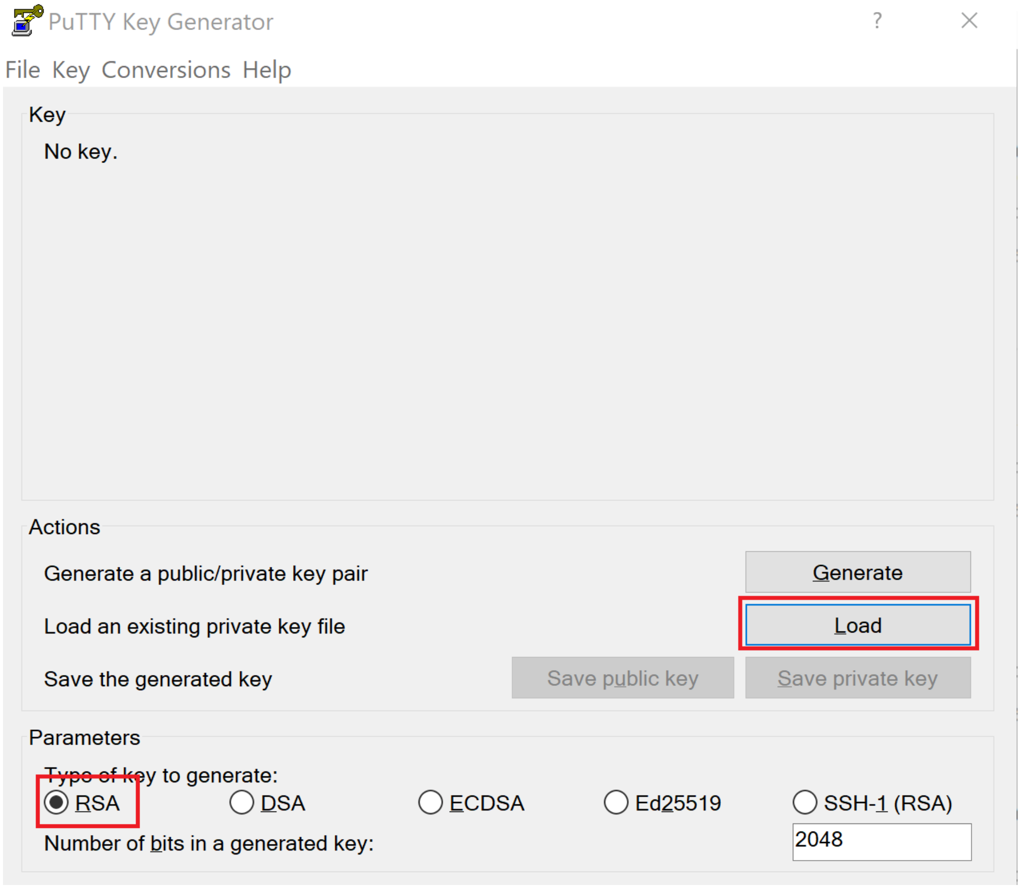
Figure 8 | Instance parameters

In order to have SSH access to the Instance we will use PuTTY. Download and install it.

In the AWS Instance page mark your instance and click “Connect”. This will bring the instructions page out. We will follow the procedure as well.

Note that we first need to convert the keys from *.pem* format to *.ppk* format as this is what PuTTY uses. This is done with PuTTYgen, which comes standard with the PuTTY package.

1. Run PuTTYgen (if you are suing Windows just type it in the start menu after installing PuTTY and you will find it).
2. In the main windows select the **Type of key to generate** as **RSA** (should be the default choice). In older versions it is named **SSH-2 RSA**.



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

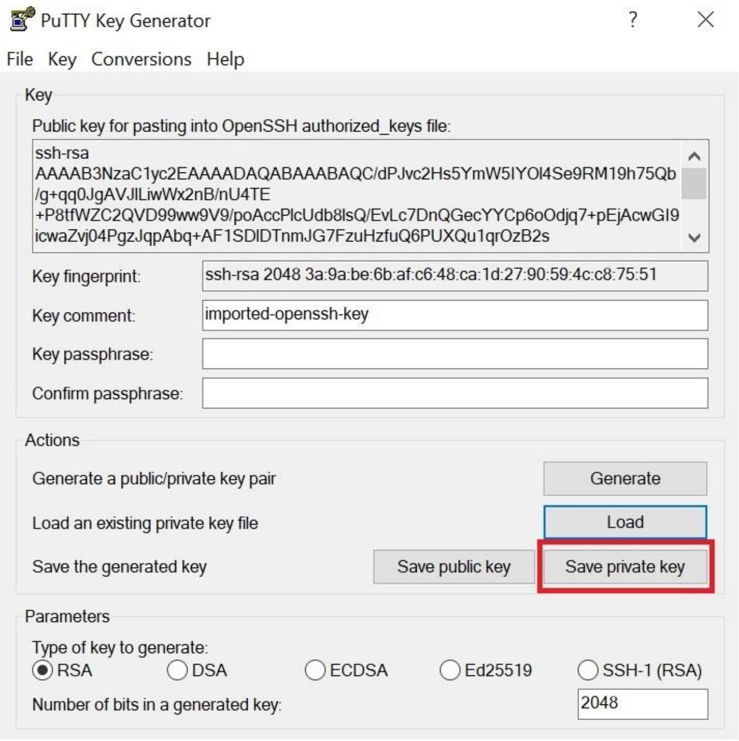
Figure 8 | PuTTYgen main window

3. Press “Load” in order to select the key files generated by AWS (make sure to select **All Files (*.*)** from the drop down menu as by default only **.ppk** files are shown

4. After successfully loading the keys you can save them in **.ppk** with the “Save private key” button. Use the same name as the original **.pem** file. The **ppk** extension will be added automatically. PuTTYgen displays a warning about saving the keys without a passphrase. Ignore it an choose **Yes.**

Note

A passphrase on a private key is an extra layer of protection. Even if your private key is discovered, it can't be used without the passphrase. The downside to using a passphrase is that it makes automation harder because human intervention is needed to log on to an instance, or to copy files to an instance.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC/dPJvc2Hs5YmW5IYOl4Se9RM19h75Qb
/g+qq0JgAVJlLiwWx2nB/nU4TE
+P8tfWZC2QVD99ww9V9/poAccPlcUdb8lsQ/EvLc7DnQGecYYCp6oOdjq7+pEjAcwGI9
icwaZvj04PgzJqpAbq+AF1SDlDTnmJG7FzuHzfuQ6PUXQu1qrOzB2s
```

Key fingerprint: ssh-rsa 2048 3a:9a:be:6b:af:c6:48:ca:1d:27:90:59:4c:c8:75:51

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

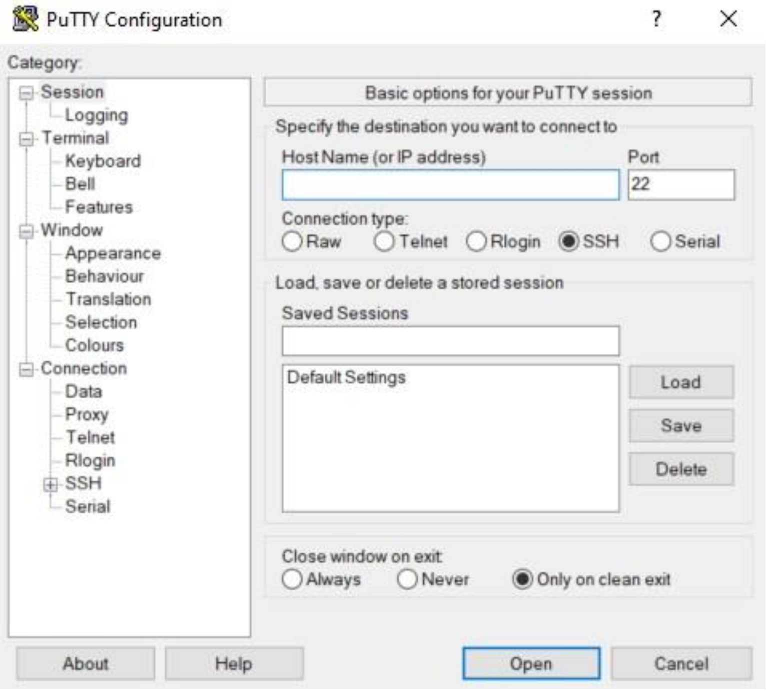
Parameters

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ Ed25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Figure 9 | PuTTYgen Saving the public key

5. As your Private Key is now in the correct format now you can create an SSH session with PuTTY. Open the client and select SSH



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit

Figure 10 | PuTTY main window

6. You need the correct **Host Name**.

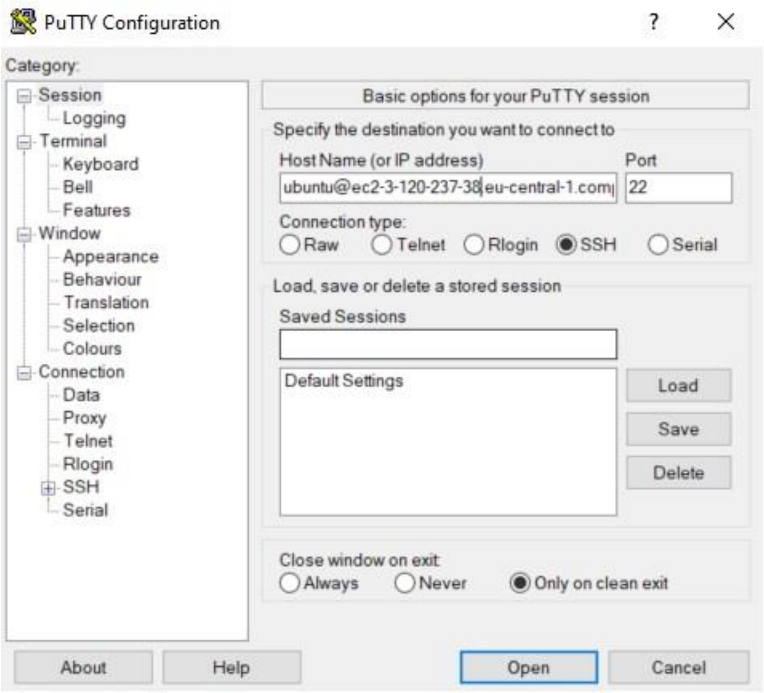
   It is in the format *user_name@public_dns_name*

   Let us look at an example:

   User_name: **ubuntu**

   Public_dns_name: **ec2-3-120-237-38.eu-central-1.compute.amazonaws.com**

   Host Name: **ubuntu@ec2-3-120-237-38.eu-central-1.compute.amazonaws.com**



Host Name (or IP address): ubuntu@ec2-3-120-237-38.eu-central-1.com

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

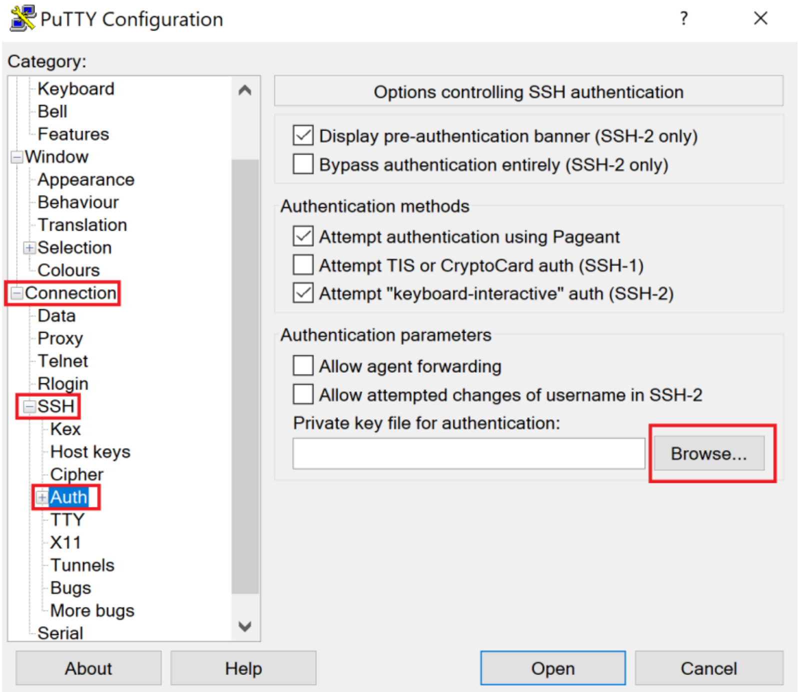
Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 11 | PuTTY main window with Host Name

7. Now we need to tell PuTTY to use our keys. In the *Category* panel expand *Connections*, expand *SSH* and select *Auth*. Click the "Browse" button and look for you **.ppk** file

   Note: If you want to save this configuration for future use go back to the *Session* tab and enter a name in the *Saved Session* text box and click *Save.*



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)

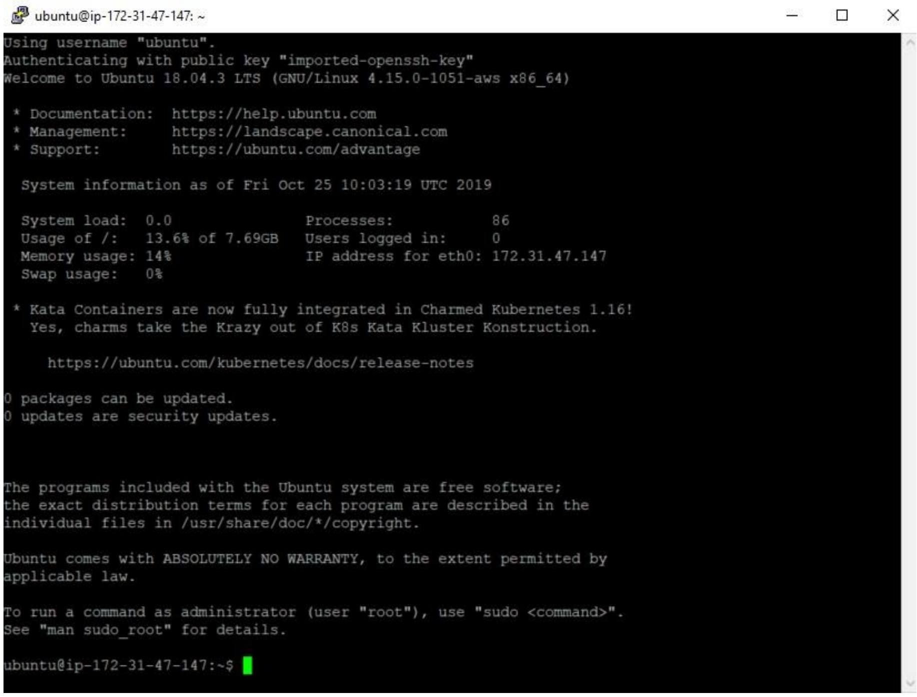
Authentication parameters

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

Private key file for authentication:

Figure 12 | PuTTY SSH Authentication

8. Click the “Open” button to initiate the session. If this is your first time connecting, PuTTY will ask for confirmation (click Yes). You should see the command line window to your instance now.



```
Using username "ubuntu".
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-1051-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Oct 25 10:03:19 UTC 2019

  System load:  0.0               Processes:           86
  Usage of /:   13.6% of 7.69GB   Users logged in:     0
  Memory usage: 14%               IP address for eth0: 172.31.47.147
  Swap usage:   0%

 * Kata Containers are now fully integrated in Charmed Kubernetes 1.16!
   Yes, charms take the Krazy out of K8s Kata Kluster Konstruction.

     https://ubuntu.com/kubernetes/docs/release-notes

0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-47-147:~$
```

Figure 12 | PuTTY SSH Command line

As a last step execute the commands in the text box below in order. This will make sure your Ubuntu is up to date:

```
sudo apt-get update
sudo apt-get upgrade
```

This concludes the tutorial.