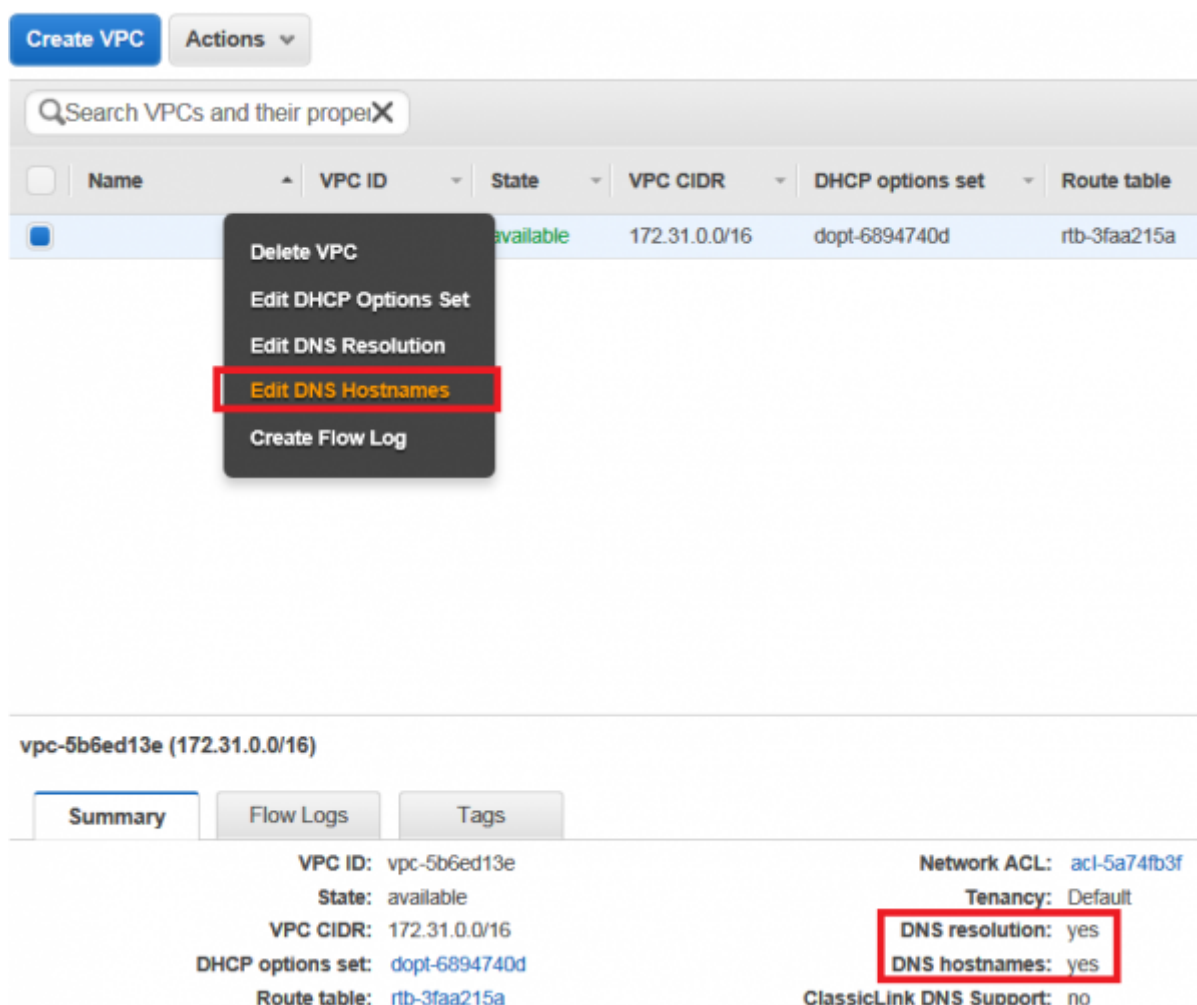


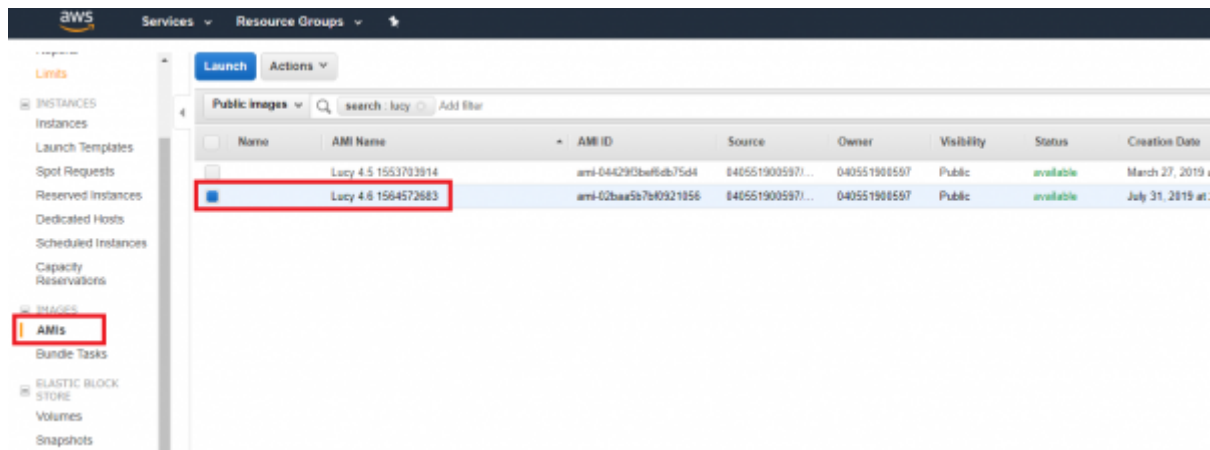
PREPARATION

- **Instance Type:** The LUCY AMI requires at least 2 GB RAM for 1000 recipients or less, 4 GB RAM for 5000 recipients or less and 8 GB RAM for 10'000 recipients or less. The minimal HDD is 250 GB. Please find your instance type here: <https://aws.amazon.com/ec2/instance-types/>
- **VPS Configuration:** You need to enable "enableDnsHostnames" in your VPC configuration in Amazon:
<http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html#vpc-dns-updating>. Otherwise you will experience an apache configuration failure due to a missing IP address in /etc/hosts. If you start new instances you need to check your VPC configuration in <https://console.aws.amazon.com/vpc/home> to verify that this setting is enabled.

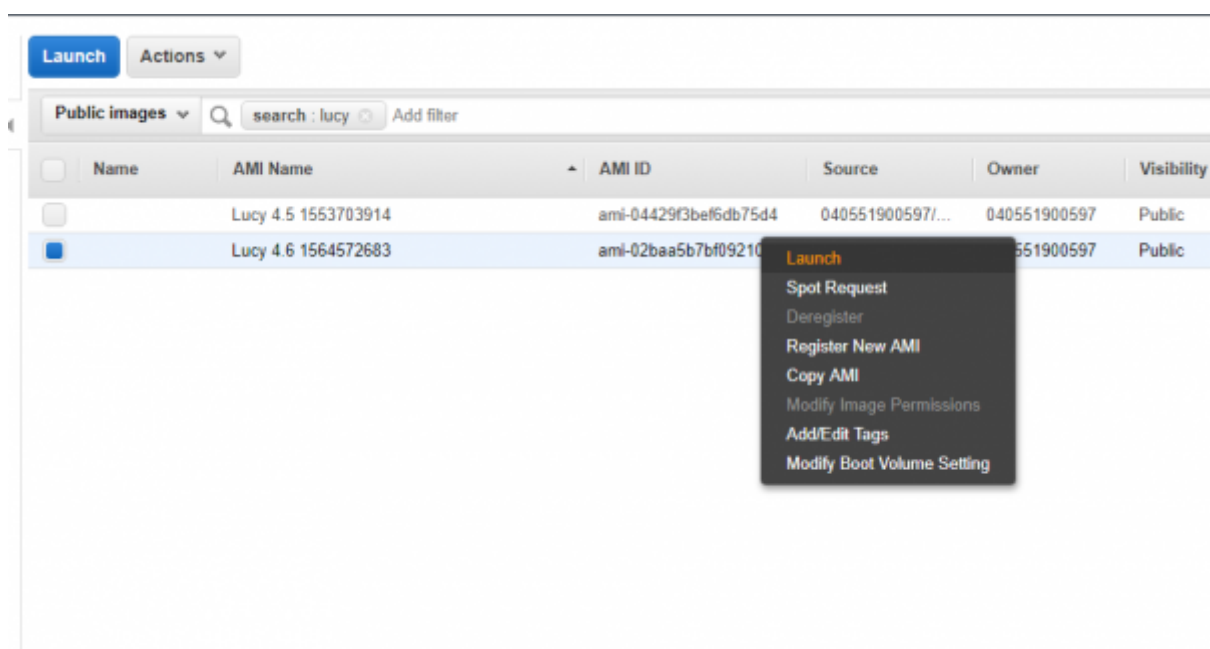


SETUP TUTORIAL

- **STEP 1: Download the AMI Image:** The AMI is available publicly via your Amazon account (use Ireland). In the AWS Management Console, open the **EC2** Dashboard. To choose an Amazon Machine Image (AMI), select the Community AMIs tab on the left hand side of the screen and search by name "**lucy**" (see the screenshot).



- **STEP 2: Launch the instance:**



- **STEP 3: Choose an Instance Type:** there are many instance types available. Please scroll down to see them all. t2.medium matches with minimal hardware requirements.

However, if you are not planning to have more than 1000 recipients, t2.small will do as well.

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.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

[Cancel](#) [Previous](#) **[Review and Launch](#)** [Next: Configure Instance Details](#)

- **STEP 4: Review Instance, Set Security group and launch:** Click on "edit security group"

AMI Details

Lucy 4.5 1564672683 - ami-4b2a25b7a98c1956
Lucy Phishing, Social Hacking and Security Awareness: <https://www.lucysecurity.com>
Instance type: x86_64 Intel Architecture

Instance Type

Instance Type	ECU	vCPU	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.medium	Variable	2	4	EBS only	-	Low to Moderate

Security Groups

Security group name: lucy-ec2-sg-3
Description: lucy-ec2-sg-3 created 2019-08-02T15:08:08.000Z

Type	Protocol	Port Range	Source	Description
This security group has no rules				

Instance Details

Storage

Tags

[Edit AMI](#) [Edit instance type](#) **[Edit security group](#)** [Edit instance details](#) [Edit storage](#) [Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

Make sure you have a security group associated with the instance that allows inbound SSH, HTTP, HTTPS & SMTP.

Edit inbound rules

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere (0.0.0.0/0)
SMTP	TCP	25	Anywhere (0.0.0.0/0)
HTTPS	TCP	443	Anywhere (0.0.0.0/0)
HTTP	TCP	80	Anywhere (0.0.0.0/0)

[Add Rule](#) [Cancel](#) [Save](#)

- **STEP 5: Create a key pair to connect:** Create a new public/private key pair for the SSH authentication and click "Download Key Pair".

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

LUCY ACCESS

Download Key Pair

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.

Cancel

Launch Instances

Note: If you are connecting from a windows host you need to convert the PEM file first. You could use PuTTY with a private key to connect to your Amazon EC2 Linux instance. To do so go through the following steps described in this guide:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>

- **STEP 6: Connect to LUCY via the public IP:** After you have launched an EC2 instance, you can connect to LUCY's public IP through SSH in order to configure the System. The public IP is visible as described in the screenshot below.

AWS									
Services Resource Groups									
EC2 Dashboard									
Events									
Tags									
Reports									
Limits									
Launch Instance Connect Actions									
Filter by tags and attributes or search by keyword									
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	
	i-07cab9b8c0bfa1e	t2.medium	eu-west-1a	running	initializing	None	ec2-34-245-138-51.eu-...	34.245.138.51	

- **STEP 7: login as admin:** After the login type "sudo su" and press enter

```
admin@ip-172-31-23-64: ~
Using username "admin".
Authenticating with public key "imported-openssh-key"
Linux ip-172-31-27-193 3.2.0-4-amd64 #1 SMP Debian 3.2.78-1 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
admin@ip-172-31-23-64:~$ sudo su
root@ip-172-31-23-64:/home/admin# python /opt/phishing/current/tools/setup/setup.py
```

- **STEP 8:** Start the image and initiate the [installation script](#). If you already have a domain name for LUCY, please make sure that you specify it within the setup script as the certificate for the administration will be based on that domain name.
- **STEP 9:** [Login](#) to LUCY with a Webbrowser. Continue the setup in the browser using the credentials provided in the setup script. If you want to install a commercial version, please provide us with the [workstation ID](#).
- **STEP 10:** Define your [default mail delivery method](#) in LUCY. In case you use the build in mail server: set the [hostname](#) for the mail server.
- **STEP 11:** Setup a [domain](#) in LUCY. This domain can be used for phishing simulations (landing pages) or the e-learning portal.
- **STEP 12:** Create a [trusted certificate](#) for the administration of LUCY.
- **STEP 13:** Create all the required administrators [users](#) in LUCY.
- **STEP 14:** [Download](#) all of the latest templates
- **STEP 15:** [Update](#) LUCY to the latest version
- **STEP 16:** Consider implementing additional [security layers](#)
- **STEP 17:** Give LUCY a [custom branding](#)
- **STEP 18:** Once you are all set you can try to [setup your first campaign](#)

Installation problem? Contact our support

In case you are planning to purchase LUCY or you are already a commercial client you can contact support@lucysecurity.com to open a ticket. We will get in touch with you within 24 hours.

Problems with sending mails within Amazon's environment

In EC2 environments we have clients reporting that there is a limitation in the amount of outbound SMTP traffic. The limit is 200 mails a day and 1 email per second.

More details here: <http://docs.aws.amazon.com/ses/latest/DeveloperGuide/limits.html>

Also, AWS doesn't support phishing simulations through SES as this is risky for their public IP to get blacklisted. If you need to send less than 200 mails per day, please use the [scheduler](#) to delay the sending.

From:
<https://wiki.lucysecurity.com/> - LUCY

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=installing_lucy_in_amazon&rev=1565272094

Last update: **2019/08/08 15:48**



