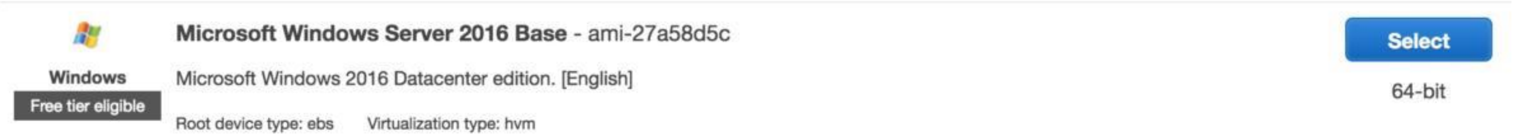
Lab-3 Launching windows Server in AWS

1. As Part of our Hands we have launched linux instance in our previous lab follow the same steps to Windows only difference is we need to select windows server AMI

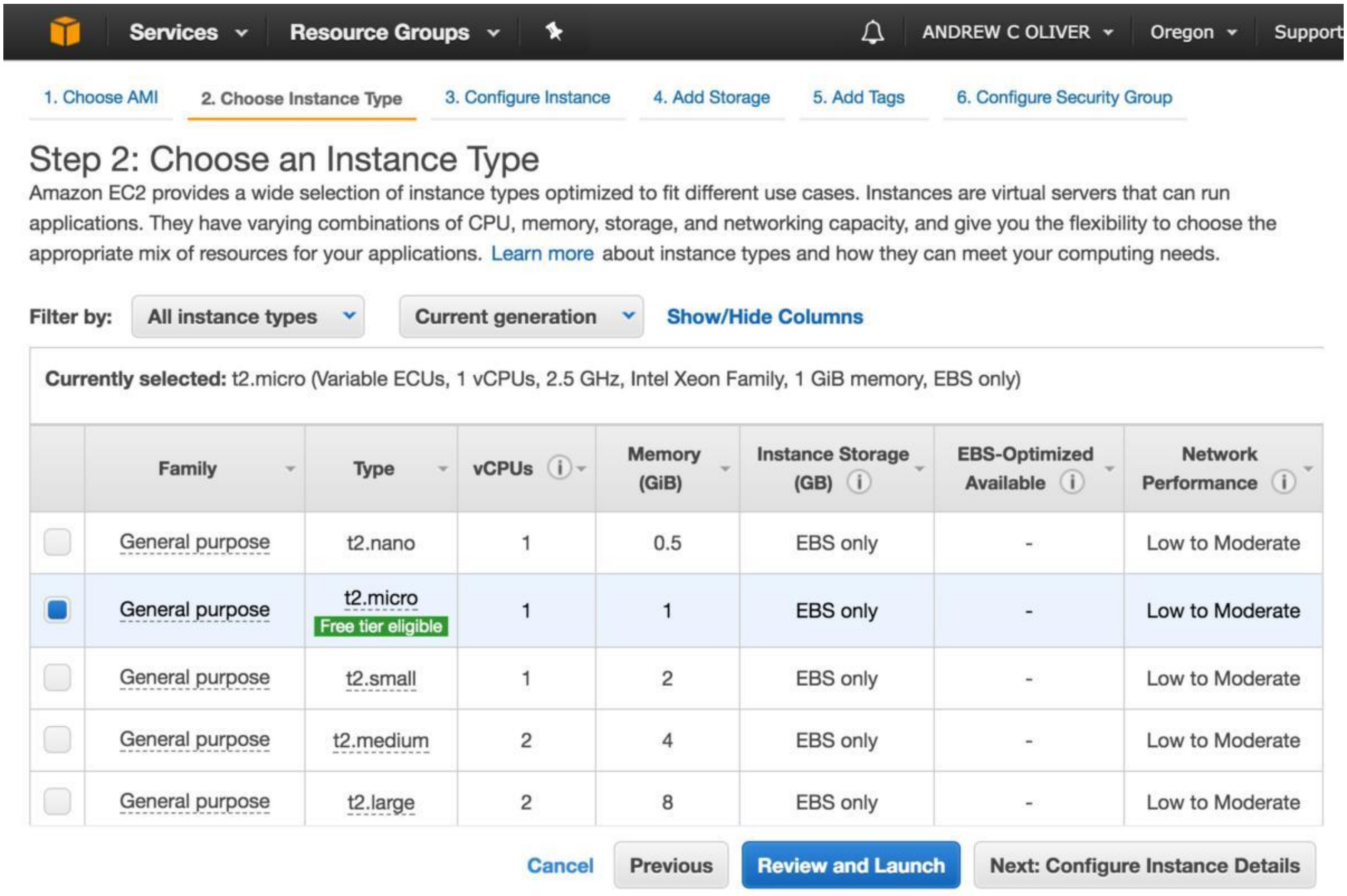


Microsoft Windows Server 2016 Base - ami-27a58d5c

Microsoft Windows 2016 Datacenter edition. [English]

Root device type: ebs Virtualization type: hvm

2. Choose Instance Type



Step 2: Choose an Instance Type

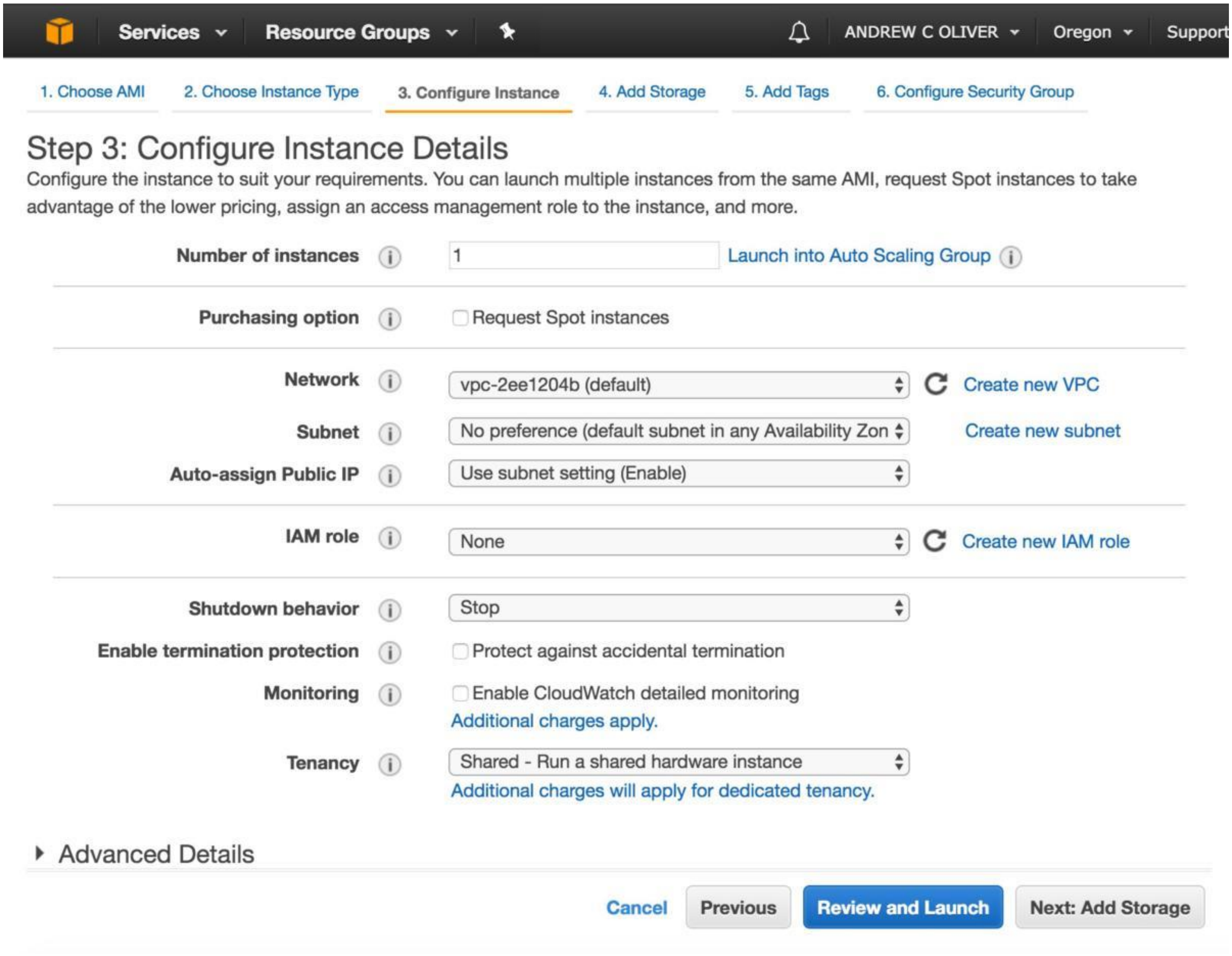
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources 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
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate
☑	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate

3. Configure Instance Details



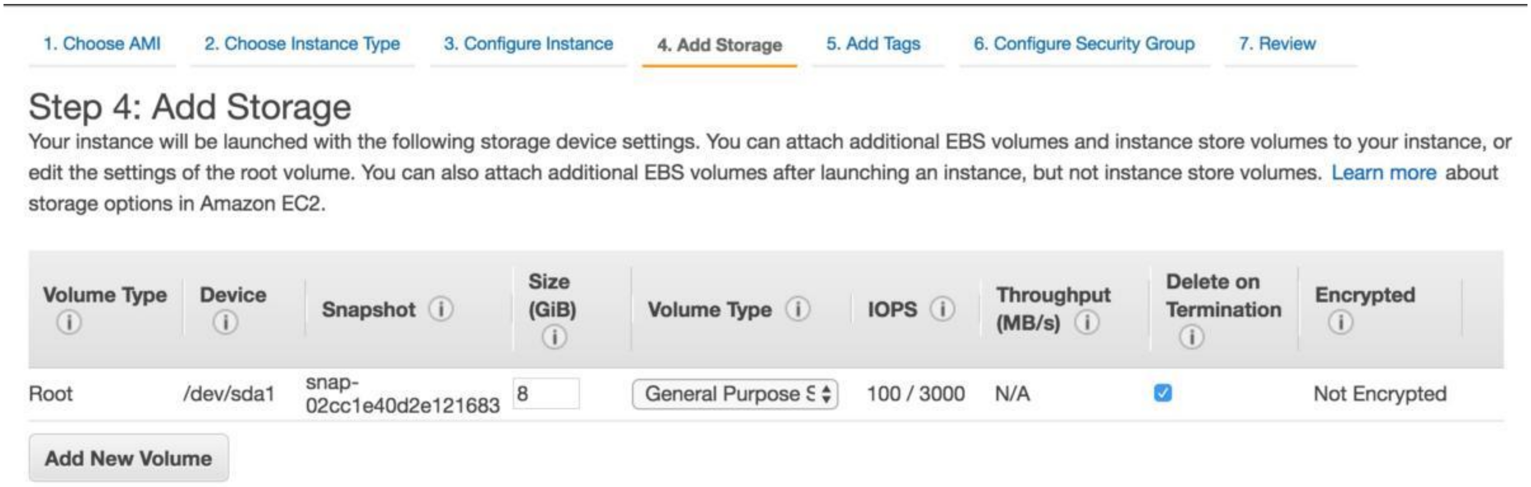
Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-2ee1204b (default) Create new VPC
Subnet	No preference (default subnet in any Availability Zon Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)
IAM role	None Create new IAM role
Shutdown behavior	Stop
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

▸ Advanced Details

4. Add Storage



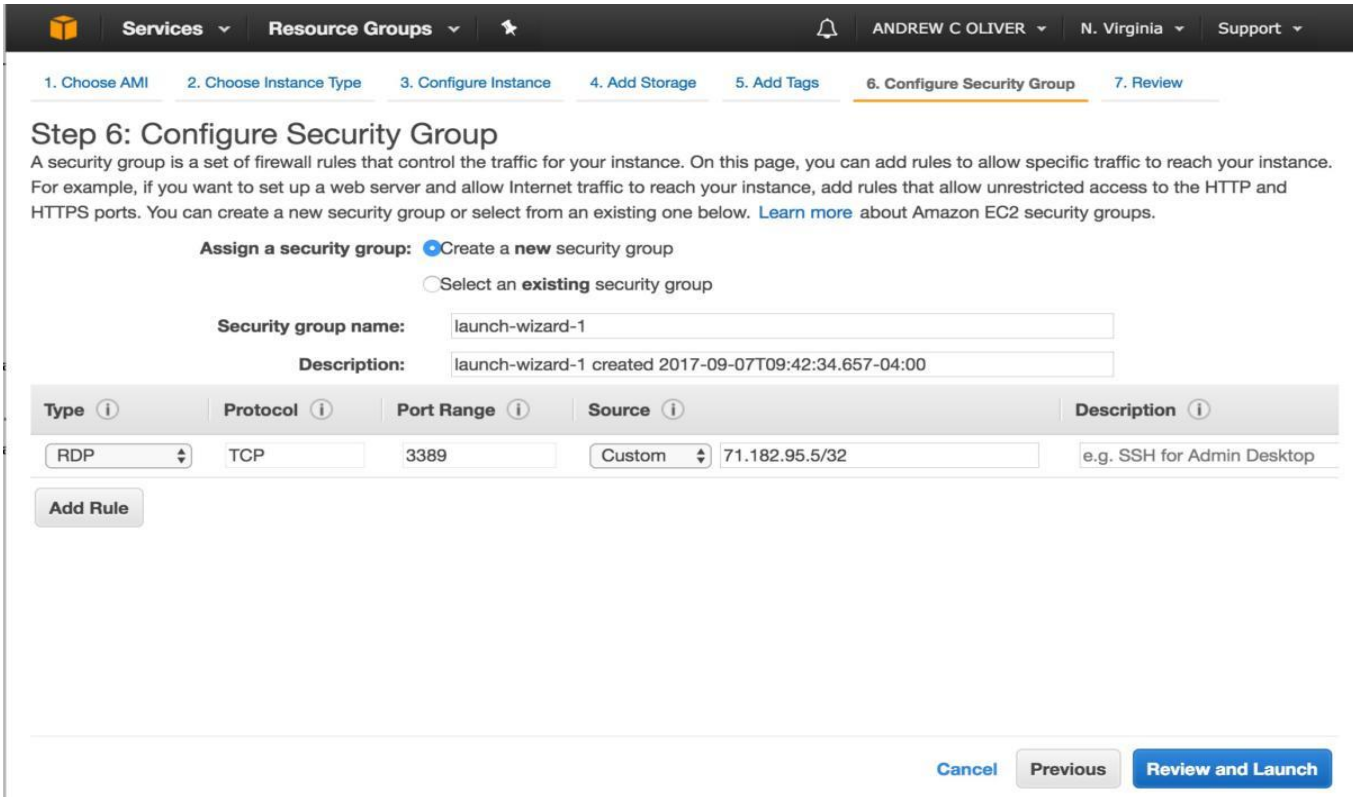
Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-02cc1e40d2e121683	8	General Purpose S	100 / 3000	N/A	☑	Not Encrypted

5. Provide naming tags

6. Create security Group with RDP open.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

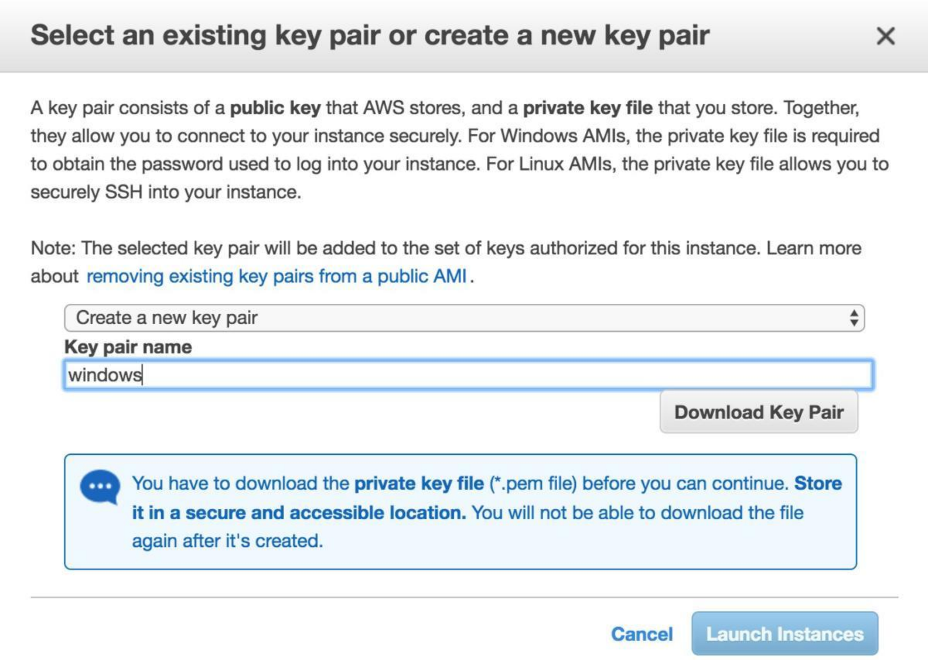
Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: launch-wizard-1

Description: launch-wizard-1 created 2017-09-07T09:42:34.657-04:00

Type	Protocol	Port Range	Source		Description
RDP	TCP	3389	Custom	71.182.95.5/32	e.g. SSH for Admin Desktop

7. Create a new 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.

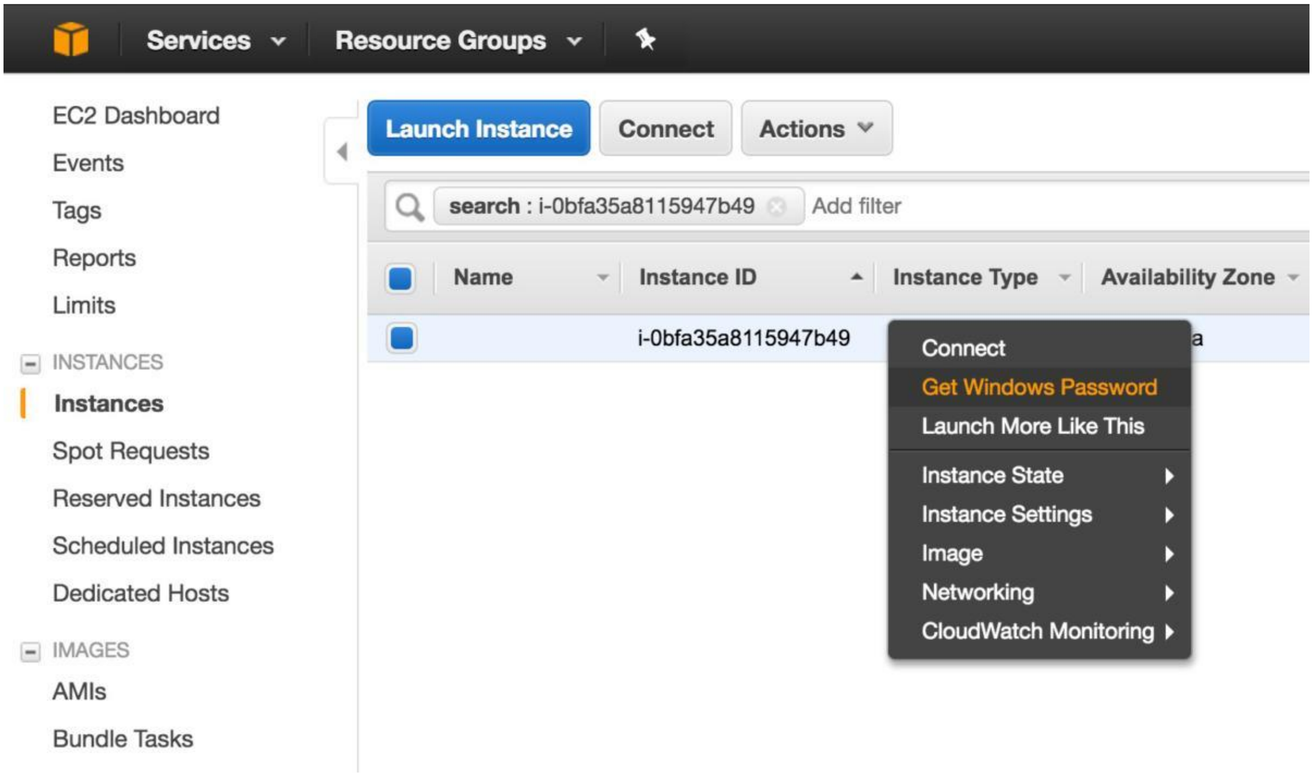
Create a new key pair

Key pair name

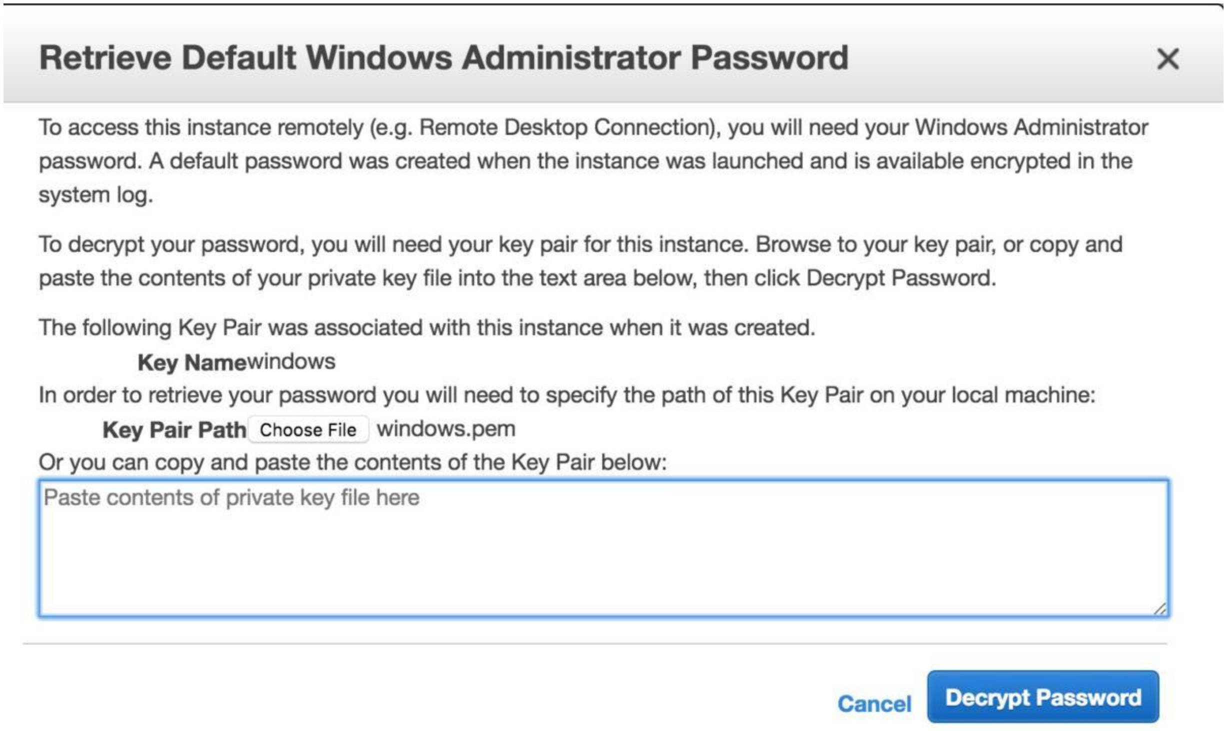
windows

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.

8. Launch instance
9. To get password right click the instance and select Get Windows Password.



10. Remember that key file? Choose it and click Decrypt Password



Retrieve Default Windows Administrator Password ×

To access this instance remotely (e.g. Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy and paste the contents of your private key file into the text area below, then click Decrypt Password.

The following Key Pair was associated with this instance when it was created.

Key Namewindows

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

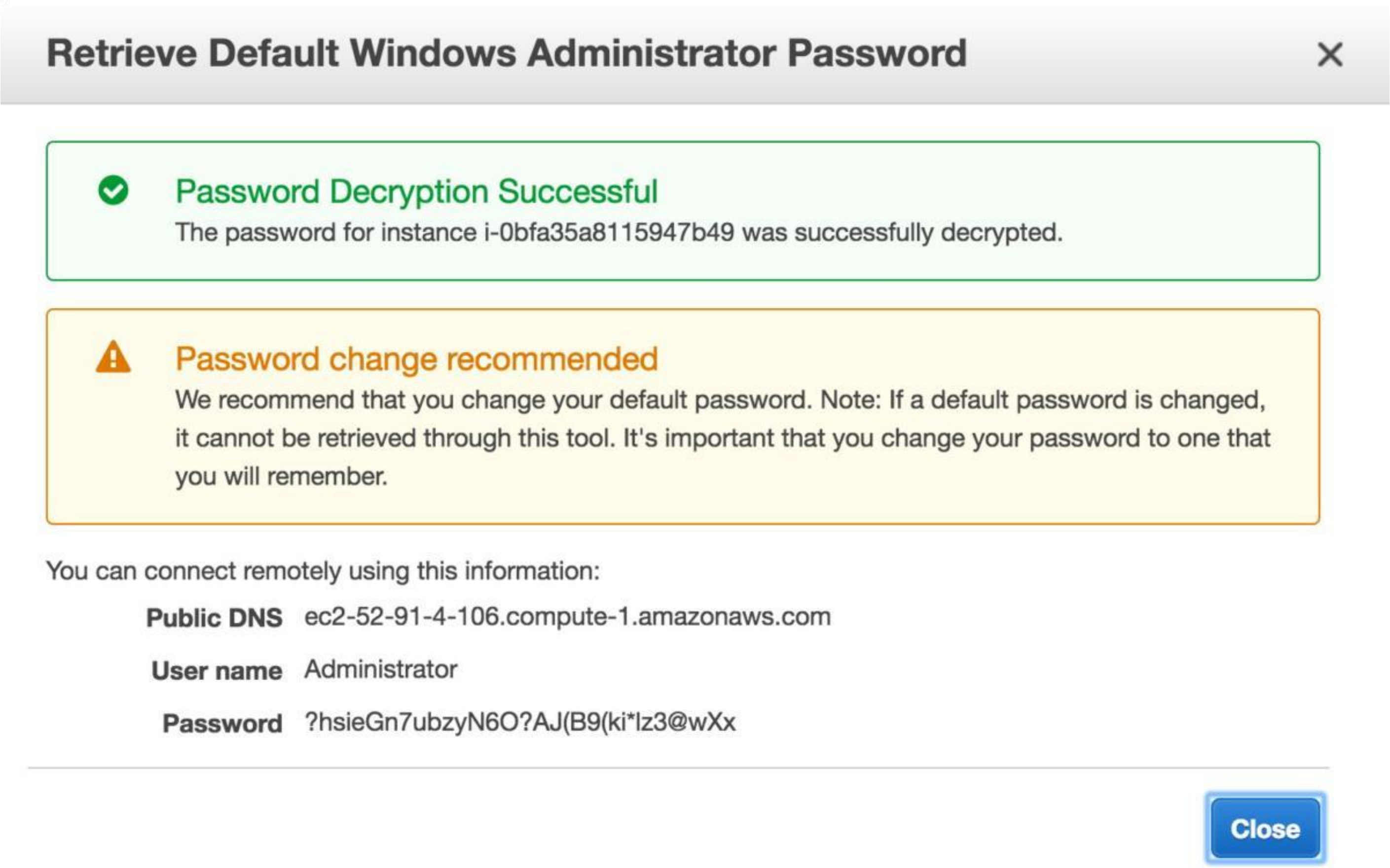
Key Pair Path Choose File windows.pem

Or you can copy and paste the contents of the Key Pair below:

Paste contents of private key file here

Cancel Decrypt Password

11. Get windows password



Retrieve Default Windows Administrator Password

Password Decryption Successful

The password for instance i-0bfa35a8115947b49 was successfully decrypted.

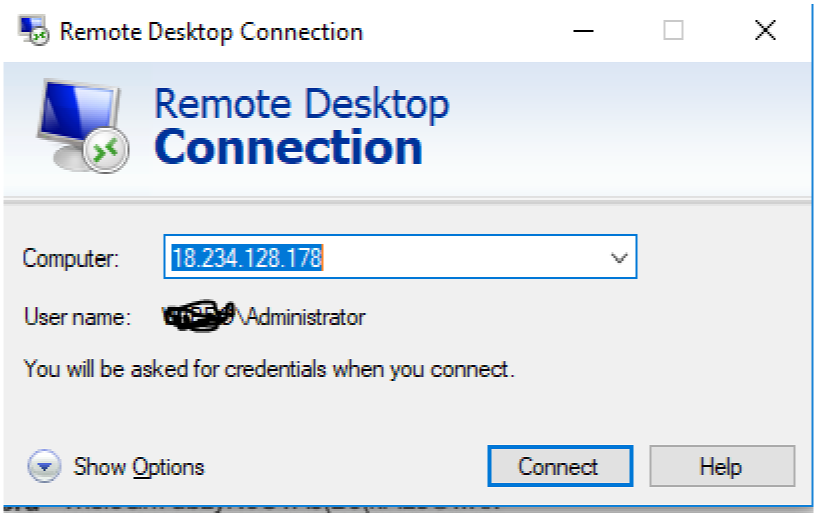
Password change recommended

We recommend that you change your default password. Note: If a default password is changed, it cannot be retrieved through this tool. It's important that you change your password to one that you will remember.

You can connect remotely using this information:

Public DNS	ec2-52-91-4-106.compute-1.amazonaws.com
User name	Administrator
Password	?hsieGn7ubzyN6O?AJ(B9(ki*Iz3@wXx

Login through Remote desktop connection.



Computer: 18.234.128.178

User name: [redacted]\Administrator

You will be asked for credentials when you connect.