**What Is Amazon EC2?**

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

**Features of Amazon EC2**

Amazon EC2 provides the following features:

* Virtual computing environments, known as *instances*
* Preconfigured templates for your instances, known as *Amazon Machine Images (AMIs)*, that package the bits you need for your server (including the operating system and additional software)
* Various configurations of CPU, memory, storage, and networking capacity for your instances, known as *instance types*
* Secure login information for your instances using *key pairs* (AWS stores the public key, and you store the private key in a secure place)
* Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as *instance store volumes*
* Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as *Amazon EBS volumes*
* Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as *regions* and *Availability Zones*
* A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using *security groups*
* Static IPv4 addresses for dynamic cloud computing, known as *Elastic IP addresses*
* Metadata, known as *tags*, that you can create and assign to your Amazon EC2 resources
* Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as *virtual private clouds* (VPCs)

**Step 1: Launch an Instance**

You can launch a Linux instance using the AWS Management Console as described in the following procedure. This tutorial is intended to help you launch your first instance quickly, so it doesn't cover all possible options. For more information about the advanced options, see [Launching an Instance](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html).

**To launch an instance**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the console dashboard, choose **Launch Instance**.
3. The **Choose an Amazon Machine Image (AMI)** page displays a list of basic configurations, called *Amazon Machine Images (AMIs)*, that serve as templates for your instance. Select the HVM edition of the Amazon Linux AMI. Notice that this AMI is marked "Free tier eligible."
4. On the **Choose an Instance Type** page, you can select the hardware configuration of your instance. Select the t2.micro type, which is selected by default. Notice that this instance type is eligible for the free tier.

**Note**

[T2 instances](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/t2-instances.html), such as t2.micro, must be launched into a VPC. If your AWS account supports EC2-Classic and you do not have a VPC in the selected region, the launch wizard creates a VPC for you and you can continue to the next step. Otherwise, the **Review and Launch** button is disabled and you must choose **Next: Configure Instance Details** and follow the directions to select a subnet.

1. Choose **Review and Launch** to let the wizard complete the other configuration settings for you.
2. On the **Review Instance Launch** page, under **Security Groups**, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:
   1. Choose **Edit security groups**.
   2. On the **Configure Security Group** page, ensure that **Select an existing security group** is selected.
   3. Select your security group from the list of existing security groups, and then choose **Review and Launch**.
3. On the **Review Instance Launch** page, choose **Launch**.
4. When prompted for a key pair, select **Choose an existing key pair**, then select the key pair that you created when getting set up.

Alternatively, you can create a new key pair. Select **Create a new key pair**, enter a name for the key pair, and then choose **Download Key Pair**. This is the only chance for you to save the private key file, so be sure to download it. Save the private key file in a safe place. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

**Caution**

Don't select the **Proceed without a key pair** option. If you launch your instance without a key pair, then you can't connect to it.

When you are ready, select the acknowledgement check box, and then choose **Launch Instances**.

1. A confirmation page lets you know that your instance is launching. Choose **View Instances** to close the confirmation page and return to the console.
2. On the **Instances** screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is pending. After the instance starts, its state changes to running and it receives a public DNS name. (If the **Public DNS (IPv4)** column is hidden, choose the Show/Hide icon in the top right corner of the page and then select **Public DNS (IPv4)**.)
3. It can take a few minutes for the instance to be ready so that you can connect to it. Check that your instance has passed its status checks; you can view this information in the **Status Checks** column.

**Step 2: Connect to Your Instance**

There are several ways to connect to a Linux instance. In this procedure, you'll connect using your browser. Alternatively, you can connect using PuTTY or an SSH client. It's also assumed that you followed the steps earlier and launched an instance from an Amazon Linux AMI, which has a specific user name. Other Linux distributions may use a different user name.

**Important**

You can't connect to your instance unless you launched it with a key pair for which you have the .pem file and you launched it with a security group that allows SSH access.

**To connect to your Linux instance using a web browser**

1. You must have Java installed and enabled in the browser. If you don't have Java already, you can contact your system administrator to get it installed, or follow the steps outlined in the following pages: [Install Java](http://java.com/en/download/help/index_installing.xml) and[Enable Java in your web browser](http://java.com/en/download/help/enable_browser.xml).
2. From the Amazon EC2 console, choose **Instances** in the navigation pane.
3. Select the instance, and then choose **Connect**.
4. Choose **A Java SSH client directly from my browser (Java required)**.
5. Amazon EC2 automatically detects the public DNS name of your instance and populates **Public DNS** for you. It also detects the key pair that you specified when you launched the instance. Complete the following, and then choose **Launch SSH Client**.
   1. In **User name**, enter ec2-user.
   2. In **Private key path**, enter the fully qualified path to your private key (.pem) file, including the key pair name.
   3. (Optional) Choose **Store in browser cache** to store the location of the private key in your browser cache. This enables Amazon EC2 to detect the location of the private key in subsequent browser sessions, until you clear your browser's cache.
6. If necessary, choose **Yes** to trust the certificate, and choose **Run** to run the MindTerm client.
7. If this is your first time running MindTerm, a series of dialog boxes asks you to accept the license agreement, confirm setup for your home directory, and confirm setup of the known hosts directory. Confirm these settings.
8. A dialog prompts you to add the host to your set of known hosts. If you do not want to store the host key information on your local computer, choose **No**.
9. A window opens and you are connected to your instance.

**Note**

If you chose **No** in the previous step, you'll see the following message, which is expected:

**Copy**

Verification of server key disabled in this session.

**Step 3: Clean Up Your Instance**

**Important**

Terminating an instance effectively deletes it; you can't reconnect to an instance after you've terminated it.

If you launched an instance that is not within the [AWS Free Tier](http://aws.amazon.com/free/), you'll stop incurring charges for that instance as soon as the instance status changes to shutting down or terminated. If you'd like to keep your instance for later, but not incur charges, you can stop the instance now and then start it again later.

**To terminate your instance**

1. In the navigation pane, choose **Instances**. In the list of instances, select the instance.
2. Choose **Actions**, then **Instance State**, and then choose **Terminate**.
3. Choose **Yes, Terminate** when prompted for confirmation.

Amazon EC2 shuts down and terminates your instance. After your instance is terminated, it remains visible on the console for a short while, and then the entry is deleted.