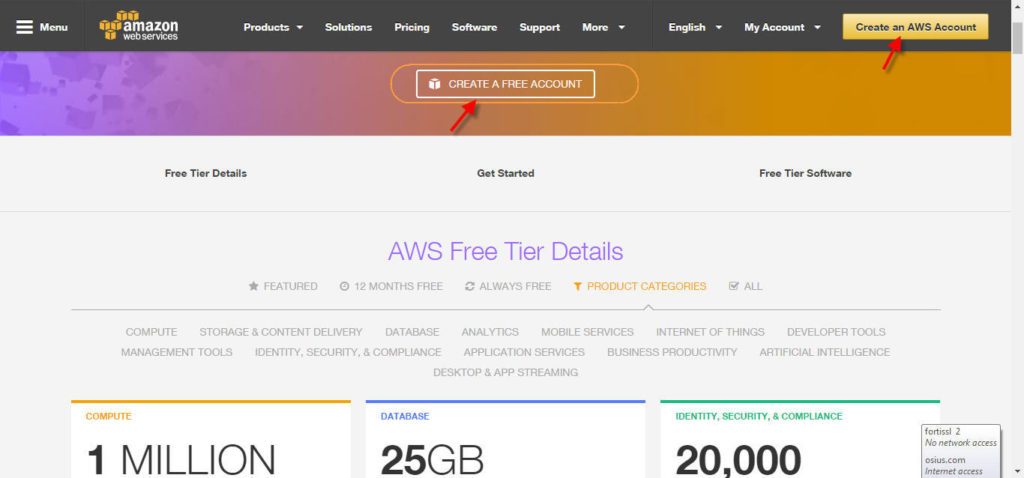


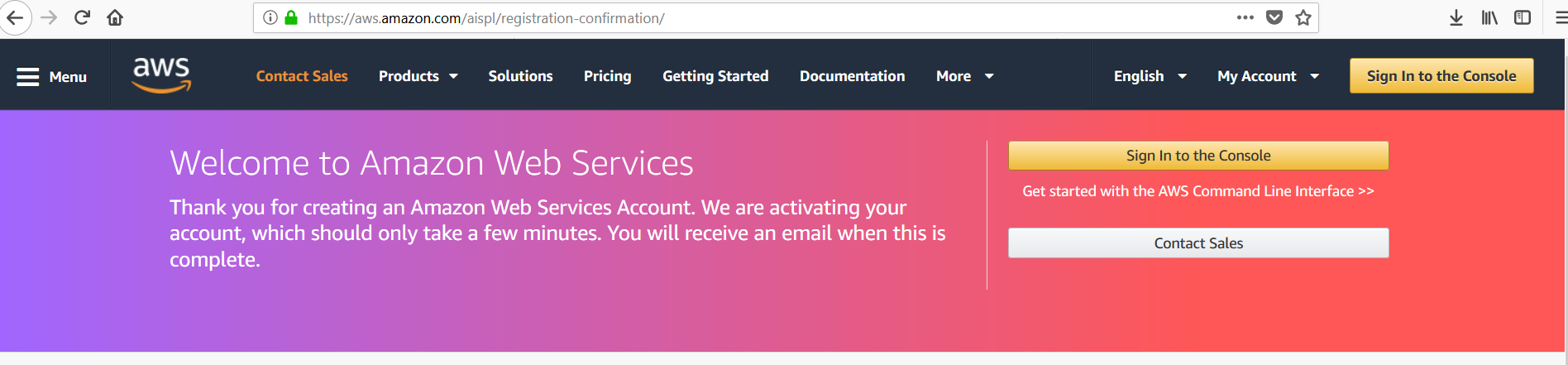
***Step By Step Guide To Create AWS Acccount And EC2 Instance***

**Step 1:  First Open your web browser and navigate to** [**https://aws.amazon.com/free/**](https://aws.amazon.com/free/)

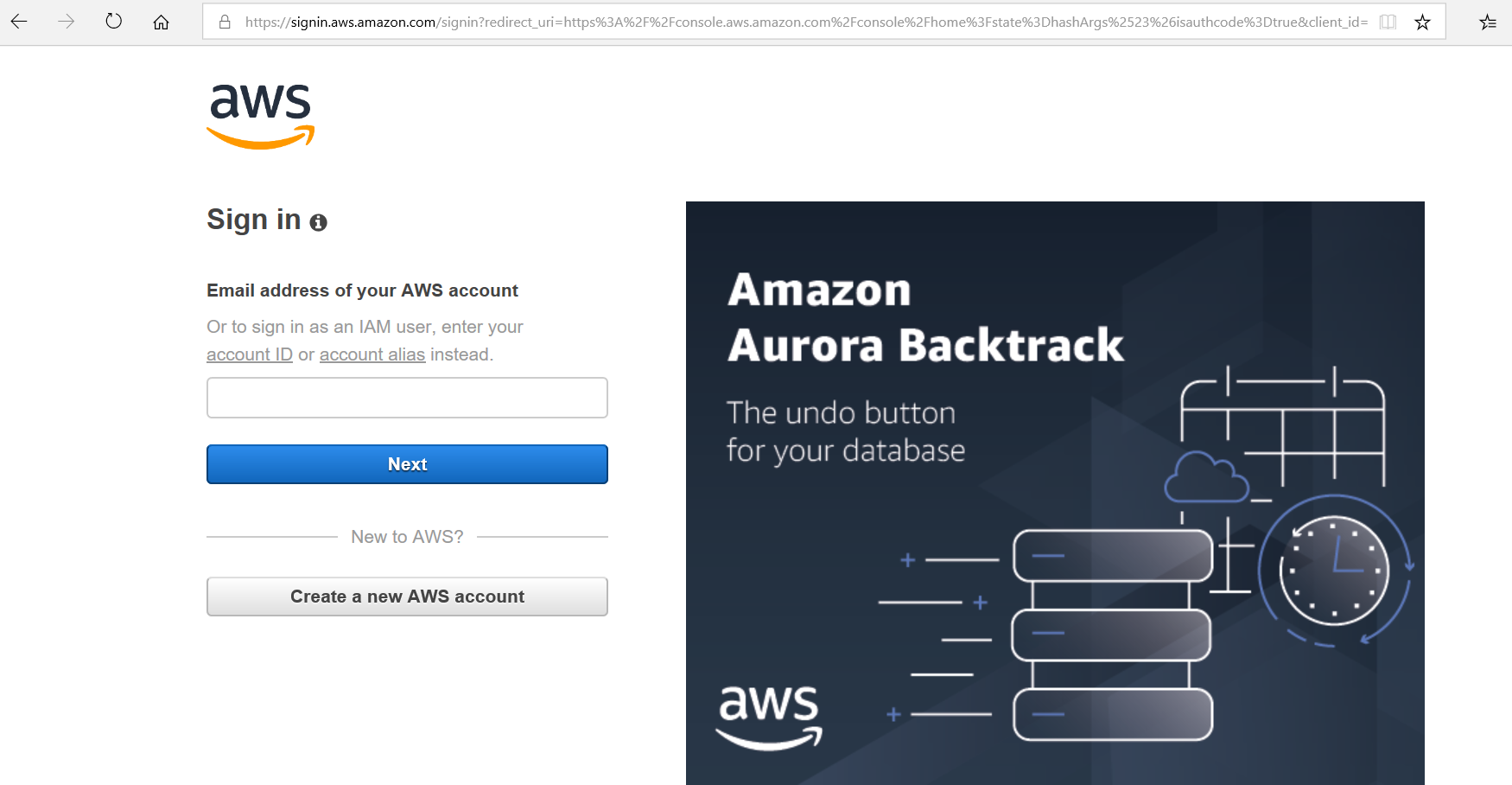
1. Click on the **“Sign Up Now” or “Create an AWS Account”** button.



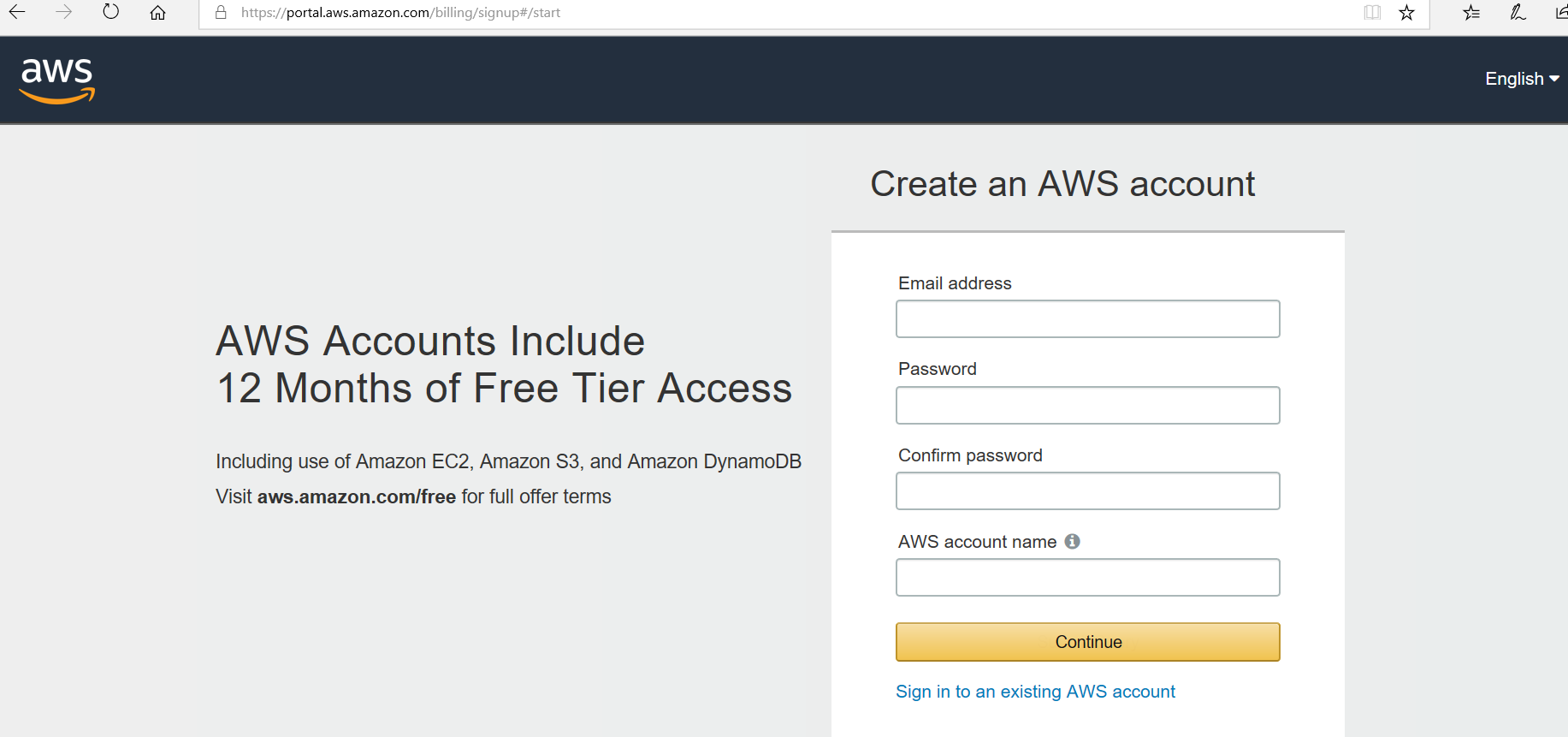
1. If you already have an Amazon store account you can use the same account to log into Amazon Web services (AWS) and then register for the free tier. If you don’t have an Amazon store account you can create a new account here by clicking on “Sign in the Console”



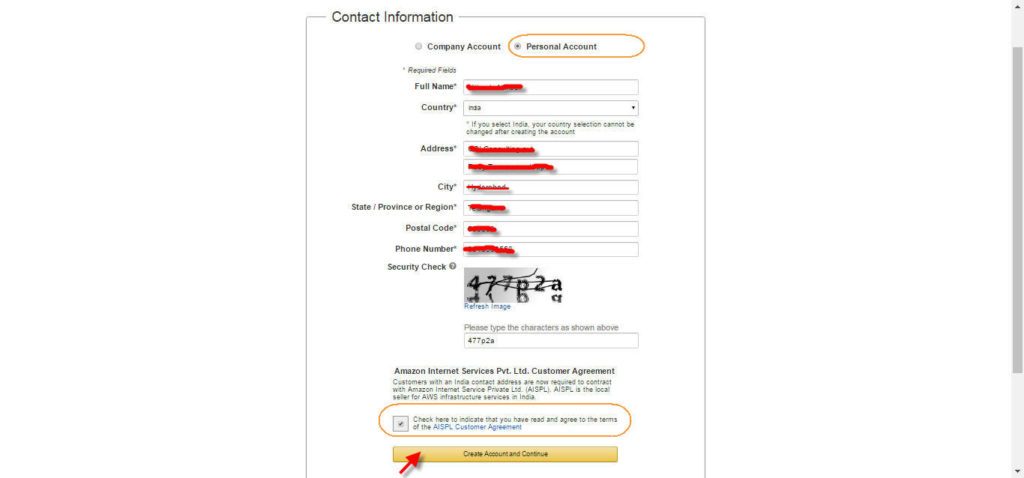
1. Click on Create New AWS account



1. **Login Credentials:** Provide the details which you want to use for login your AWS account.



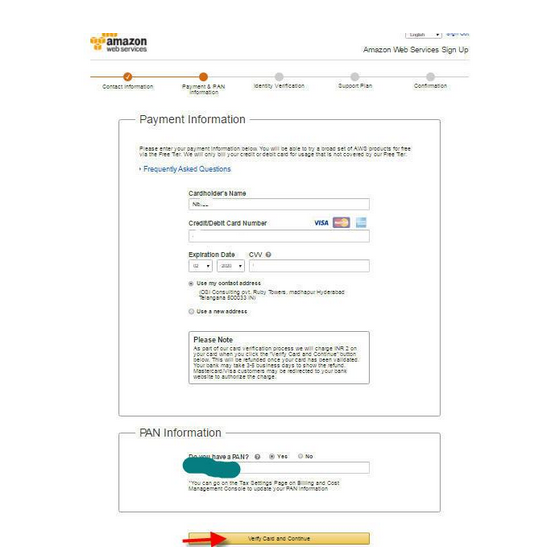
**Step 2:** **Contact Information**

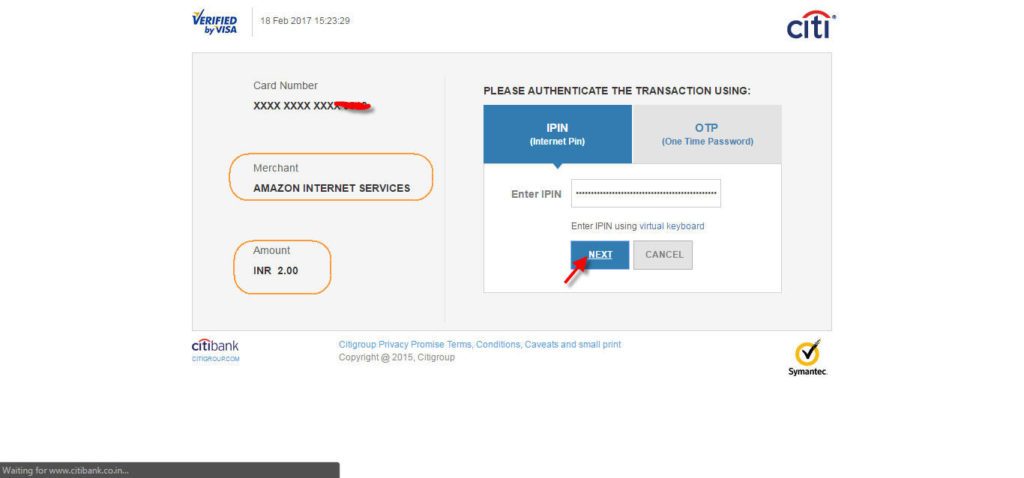
Select your AWS type, then Fill the correct information to validate your account if you’re going to create personal use then click on “personal Account” else use “company Account”.

Make sure provide proper contact details and mobile no. to get the call from AWS for verification. After completed the form enters the captcha code and click on “create the account and continue”.

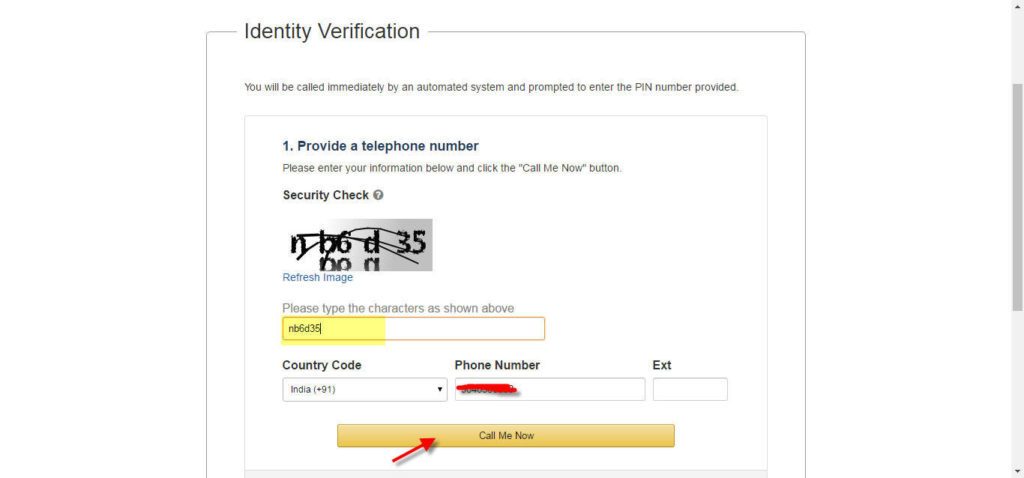
**Step 3: Payment and PAN information:**

In this step, you must fill in your credit card info and billing address. If you have PAN then fill those details here.

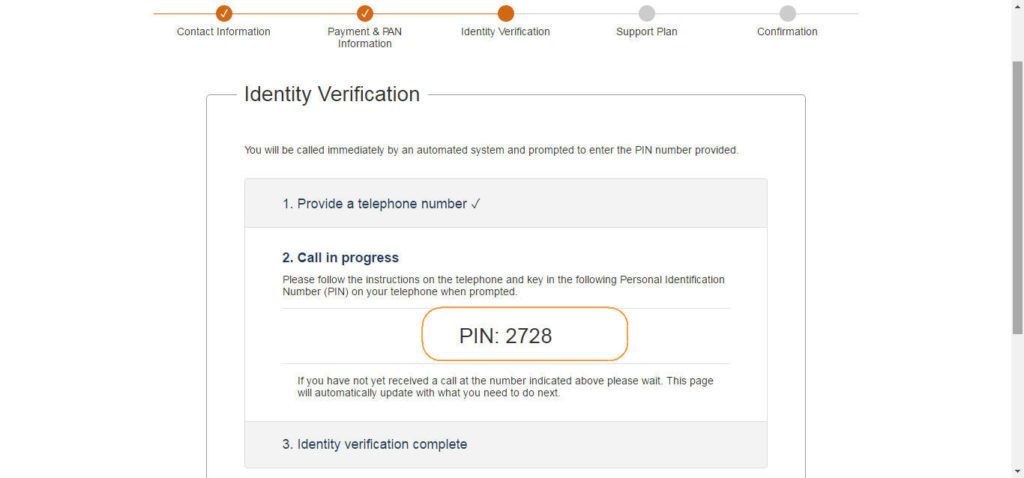


**Step4:** In this step, it will take you to the payment gateway to validate your payment information and for your credit card verification Amazon will charge the minimal price based on Country. Here I have provided India, so Amazon charged **2 INR**.

**Step 5: Identity verification**

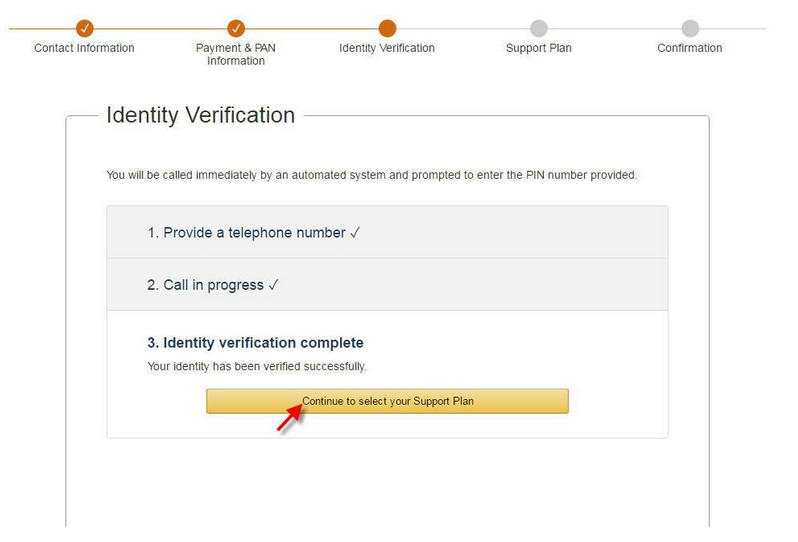
Here you will be taken to an identity verification page that will already have your phone number, so you just have to click the “**Call me now**” button to continue the process.

**Step 6: Personal Identification number**

After receiving a call from AWS, the next page will show your **PIN #** while a call is made to the phone number you have provided.  When it ask you to type your **PIN #** the webpage is providing you for identity verification purposes.

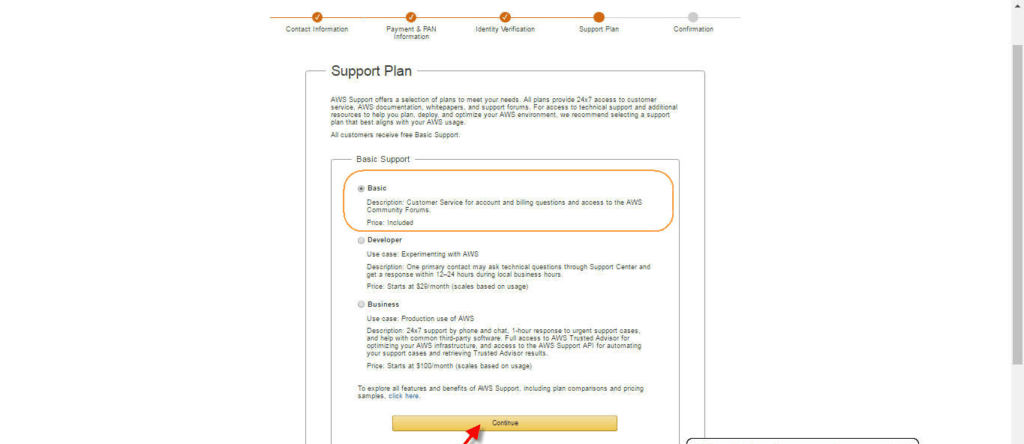
**Step 7: Identity Verification complete**

Once your verification is complete just click the “**Continue**” button

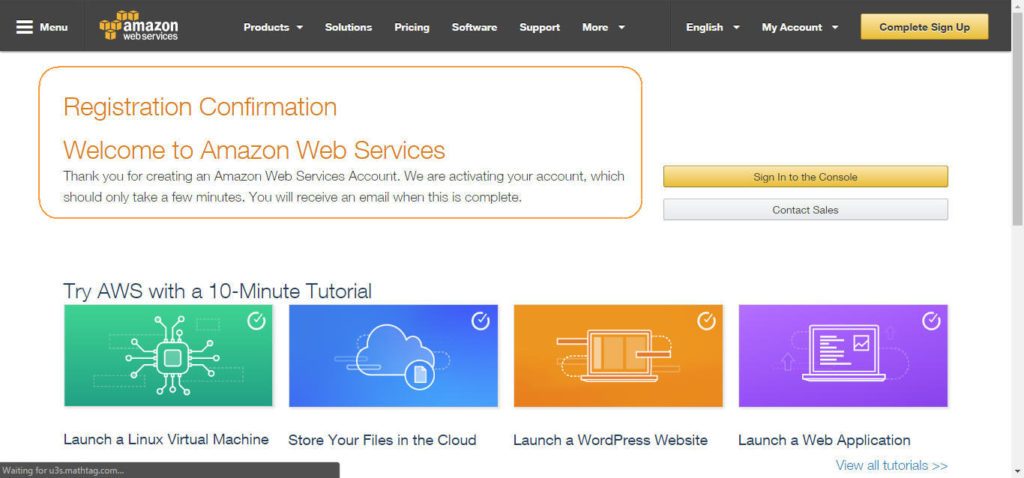


**Step 8: Support plan**

AWS support offers a selection of plans to meet your business needs. Select your suitable plan then click continue.

**Note:** All customers receive free basic support.

**Step 9: Registration Confirmation page.**

Once you completed all the above steps and process. You’ll get the confirmation page like below**.** Now your account will be processed for activation. It may take somewhere between 30 minutes to 1 hour for you to receive an email confirmation that your Amazon Cloud Services account has been activated.

**Setting Up with Amazon EC2**

If you've already signed up for Amazon Web Services (AWS), you can start using Amazon EC2 immediately. You can open the Amazon EC2 console, choose **Launch Instance**, and follow the steps in the launch wizard to launch your first instance.

If you haven't signed up for AWS yet, or if you need assistance launching your first instance, complete the following tasks to get set up to use Amazon EC2:

1. [Sign Up for AWS](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html#sign-up-for-aws)
2. [Create an IAM User](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html#create-an-iam-user)
3. [Create a Key Pair](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html#create-a-key-pair)
4. [Create a Virtual Private Cloud (VPC)](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html#create-a-vpc)
5. [Create a Security Group](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html#create-a-base-security-group)

**Sign Up for AWS**

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon EC2. You are charged only for the services that you use.

With Amazon EC2, you pay only for what you use. If you are a new AWS customer, you can get started with Amazon EC2 for free. For more information, see [AWS Free Tier](https://aws.amazon.com/free/).

If you have an AWS account already, skip to the next task. If you don't have an AWS account, use the following procedure to create one.

**To create an AWS account**

1. Open <https://aws.amazon.com/>, and then choose **Create an AWS Account**.

Note

This might be unavailable in your browser if you previously signed into the AWS Management Console. In that case, choose **Sign in to a different account**, and then choose **Create a new AWS account**.

1. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Note your AWS account number, because you'll need it for the next task.

**Create an IAM User**

Services in AWS, such as Amazon EC2, require that you provide credentials when you access them, so that the service can determine whether you have permission to access its resources. The console requires your password. You can create access keys for your AWS account to access the command line interface or API. However, we don't recommend that you access AWS using the credentials for your AWS account; we recommend that you use AWS Identity and Access Management (IAM) instead. Create an IAM user, and then add the user to an IAM group with administrative permissions or grant this user administrative permissions. You can then access AWS using a special URL and the credentials for the IAM user.

If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console. If you aren't familiar with using the console, see [Working with the AWS Management Console](http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/getting-started.html) for an overview.

**To create an IAM user for yourself and add the user to an Administrators group**

1. Use your AWS account email address and password to sign in as the [*AWS account root user*](http://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html) to the IAM console at <https://console.aws.amazon.com/iam/>.

Note

We strongly recommend that you adhere to the best practice of using the **Administrator** IAM user below and securely lock away the root user credentials. Sign in as the root user only to perform a few [account and service management tasks](http://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html).

1. In the navigation pane of the console, choose **Users**, and then choose **Add user**.
2. For **User name**, type **Administrator**.
3. Select the check box next to **AWS Management Console access**, select **Custom password**, and then type the new user's password in the text box. You can optionally select **Require password reset** to force the user to create a new password the next time the user signs in.
4. Choose **Next: Permissions**.
5. On the **Set permissions** page, choose **Add user to group**.
6. Choose **Create group**.
7. In the **Create group** dialog box, for **Group name** type **Administrators**.
8. For **Filter policies**, select the check box for **AWS managed - job function**.
9. In the policy list, select the check box for **AdministratorAccess**. Then choose **Create group**.
10. Back in the list of groups, select the check box for your new group. Choose **Refresh** if necessary to see the group in the list.
11. Choose **Next: Review** to see the list of group memberships to be added to the new user. When you are ready to proceed, choose **Create user**.

You can use this same process to create more groups and users, and to give your users access to your AWS account resources. To learn about using policies to restrict users' permissions to specific AWS resources, go to [Access Management](http://docs.aws.amazon.com/IAM/latest/UserGuide/access.html) and [Example Policies](http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_examples.html).

To sign in as this new IAM user, sign out of the AWS console, then use the following URL, where *your\_aws\_account\_id* is your AWS account number without the hyphens (for example, if your AWS account number is 1234-5678-9012, your AWS account ID is 123456789012):

https://*your\_aws\_account\_id*.signin.aws.amazon.com/console/

Enter the IAM user name (not your email address) and password that you just created. When you're signed in, the navigation bar displays "*your\_user\_name* @ *your\_aws\_account\_id*".

If you don't want the URL for your sign-in page to contain your AWS account ID, you can create an account alias. From the IAM console, choose **Dashboard** in the navigation pane. From the dashboard, choose **Customize** and enter an alias such as your company name. To sign in after you create an account alias, use the following URL:

https://*your\_account\_alias*.signin.aws.amazon.com/console/

To verify the sign-in link for IAM users for your account, open the IAM console and check under **IAM users sign-in link** on the dashboard.

For more information about IAM, see [IAM and Amazon EC2](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/UsingIAM.html#intro-to-iam).

**Create a Key Pair**

AWS uses public-key cryptography to secure the login information for your instance. A Linux instance has no password; you use a key pair to log in to your instance securely. You specify the name of the key pair when you launch your instance, then provide the private key when you log in using SSH.

If you haven't created a key pair already, you can create one using the Amazon EC2 console. Note that if you plan to launch instances in multiple regions, you'll need to create a key pair in each region. For more information about regions, see [Regions and Availability Zones](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html).

**To create a key pair**

1. Sign in to AWS using the URL that you created in the previous section.
2. From the AWS dashboard, choose **EC2** to open the Amazon EC2 console.
3. From the navigation bar, select a region for the key pair. You can select any region that's available to you, regardless of your location. However, key pairs are specific to a region; for example, if you plan to launch an instance in the US East (Ohio) Region, you must create a key pair for the instance in the US East (Ohio) Region.


      Select a region
     

1. In the navigation pane, under **NETWORK & SECURITY**, choose **Key Pairs**.

Tip

The navigation pane is on the left side of the console. If you do not see the pane, it might be minimized; choose the arrow to expand the pane. You may have to scroll down to see the **Key Pairs** link.


      Open the key pairs page
     

1. Choose **Create Key Pair**.
2. Enter a name for the new key pair in the **Key pair name** field of the **Create Key Pair** dialog box, and then choose **Create**. Use a name that is easy for you to remember, such as your IAM user name, followed by -key-pair, plus the region name. For example, *me*-key-pair-*useast2*.
3. The private key file is automatically downloaded by your browser. The base file name is the name you specified as the name of your key pair, and the file name extension is .pem. Save the private key file in a safe place.

Important

This is the only chance for you to save the private key file. 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.

1. If you will use an SSH client on a Mac or Linux computer to connect to your Linux instance, use the following command to set the permissions of your private key file so that only you can read it.

**chmod 400 *your\_user\_name*-key-pair-*region\_name*.pem**

If you do not set these permissions, then you cannot connect to your instance using this key pair. For more information, see [Error: Unprotected Private Key File](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html#troubleshoot-unprotected-key).

For more information, see [Amazon EC2 Key Pairs](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html).

**To connect to your instance using your key pair**

To connect to your Linux instance from a computer running Mac or Linux, you'll specify the .pem file to your SSH client with the -i option and the path to your private key. To connect to your Linux instance from a computer running Windows, you can use either MindTerm or PuTTY. If you plan to use PuTTY, you'll need to install it and use the following procedure to convert the .pem file to a .ppk file.

**(Optional) To prepare to connect to a Linux instance from Windows using PuTTY**

1. Download and install PuTTY from <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. Be sure to install the entire suite.
2. Start PuTTYgen (for example, from the **Start** menu, choose **All Programs > PuTTY > PuTTYgen**).
3. Under **Type of key to generate**, choose **RSA**.


      SSH-2 RSA key in PuTTYgen
     

1. Choose **Load**. By default, PuTTYgen displays only files with the extension .ppk. To locate your .pem file, select the option to display files of all types.


      Select all file types
     

1. Select the private key file that you created in the previous procedure and choose **Open**. Choose **OK** to dismiss the confirmation dialog box.
2. Choose **Save private key**. PuTTYgen displays a warning about saving the key without a passphrase. Choose **Yes**.
3. Specify the same name for the key that you used for the key pair. PuTTY automatically adds the .ppk file extension.

**Create a Virtual Private Cloud (VPC)**

Amazon VPC enables you to launch AWS resources into a virtual network that you've defined. If you have a default VPC, you can skip this section and move to the next task, [Create a Security Group](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/get-set-up-for-amazon-ec2.html#create-a-base-security-group). To determine whether you have a default VPC, see [Supported Platforms in the Amazon EC2 Console](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-supported-platforms.html#console-updates). Otherwise, you can create a nondefault VPC in your account using the steps below.

Important

If your account supports EC2-Classic in a region, then you do not have a default VPC in that region. T2 instances must be launched into a VPC.

**To create a nondefault VPC**

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. From the navigation bar, select a region for the VPC. VPCs are specific to a region, so you should select the same region in which you created your key pair.
3. On the VPC dashboard, choose **Create VPC**.
4. On the **Step 1: Select a VPC Configuration** page, ensure that **VPC with a Single Public Subnet** is selected, and choose **Select**.
5. On the **Step 2: VPC with a Single Public Subnet** page, enter a friendly name for your VPC in the **VPC name** field. Leave the other default configuration settings, and choose **Create VPC**. On the confirmation page, choose **OK**.

For more information about Amazon VPC, see [What is Amazon VPC?](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/) in the *Amazon VPC User Guide*.

**Create a Security Group**

Security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level. You must add rules to a security group that enable you to connect to your instance from your IP address using SSH. You can also add rules that allow inbound and outbound HTTP and HTTPS access from anywhere.

Note that if you plan to launch instances in multiple regions, you'll need to create a security group in each region. For more information about regions, see [Regions and Availability Zones](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html).

**Prerequisites**

You'll need the public IPv4 address of your local computer. The security group editor in the Amazon EC2 console can automatically detect the public IPv4 address for you. Alternatively, you can use the search phrase "what is my IP address" in an Internet browser, or use the following service: [Check IP](http://checkip.amazonaws.com/). If you are connecting through an Internet service provider (ISP) or from behind a firewall without a static IP address, you need to find out the range of IP addresses used by client computers.

**To create a security group with least privilege**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.

Tip

Alternatively, you can use the Amazon VPC console to create a security group. However, the instructions in this procedure don't match the Amazon VPC console. Therefore, if you switched to the Amazon VPC console in the previous section, either switch back to the Amazon EC2 console and use these instructions, or use the instructions in [Set Up a Security Group for Your VPC](http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/SecurityGroup.html) in the *Amazon VPC Getting Started Guide*.

1. From the navigation bar, select a region for the security group. Security groups are specific to a region, so you should select the same region in which you created your key pair.


      Select a region
     

1. Choose **Security Groups** in the navigation pane.
2. Choose **Create Security Group**.
3. Enter a name for the new security group and a description. Use a name that is easy for you to remember, such as your IAM user name, followed by \_SG\_, plus the region name. For example, *me*\_SG\_*uswest2*.
4. In the **VPC** list, select your VPC. If you have a default VPC, it's the one that is marked with an asterisk (\*).

Note

If your account supports EC2-Classic, select the VPC that you created in the previous task.

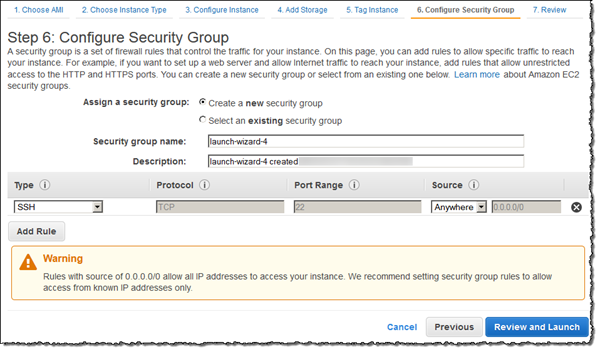
1. On the **Inbound** tab, create the following rules (choose **Add Rule** for each new rule), and then choose **Create**:
   * Choose **HTTP** from the **Type** list, and make sure that **Source** is set to **Anywhere** (0.0.0.0/0).
   * Choose **HTTPS** from the **Type** list, and make sure that **Source** is set to **Anywhere** (0.0.0.0/0).
   * Choose **SSH** from the **Type** list. In the **Source** box, choose **My IP** to automatically populate the field with the public IPv4 address of your local computer. Alternatively, choose **Custom** and specify the public IPv4 address of your computer or network in CIDR notation. To specify an individual IP address in CIDR notation, add the routing suffix /32, for example, 203.0.113.25/32. If your company allocates addresses from a range, specify the entire range, such as 203.0.113.0/24.

Warning

For security reasons, we don't recommend that you allow SSH access from all IPv4 addresses (0.0.0.0/0) to your instance, except for testing purposes and only for a short time.

**To launch the EC2 instance**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. Choose **Launch Instance**.
3. In **Step 1: Choose an Amazon Machine Image (AMI)**, find an Amazon Linux AMI at the top of the list and choose **Select**.
4. In **Step 2: Choose an Instance Type**, choose **Next: Configure Instance Details**.
5. In **Step 3: Configure Instance Details**, choose **Network**, and then choose the entry for your default VPC. It should look something like vpc-xxxxxxx (172.31.0.0/16) (default).
   1. Choose **Subnet**, and then choose a subnet in any Availability Zone.
   2. Choose **Next: Add Storage**.
6. Choose **Next: Tag Instance**. Name your instance and choose **Next: Configure Security Group**.
7. In **Step 6: Configure Security Group**, review the contents of this page, ensure that **Assign a security group** is set to **Create a new security group**, and verify that the inbound rule being created has the following default values.
   1. **Type:** SSH
   2. **Protocol:** TCP
   3. **Port Range:** 22
   4. **Source:** Anywhere 0.0.0.0/0



1. NoteYou can configure the EFS file system to mount on your EC2 instance automatically. For more information, see [Configuring an EFS File System to Mount Automatically at EC2 Instance Launch](https://docs.aws.amazon.com/efs/latest/ug/mount-fs-auto-mount-onreboot.html#mount-fs-auto-mount-on-creation).
2. Choose **Review and Launch**.
3. Choose **Launch**.
4. Select the check box for the key pair that you created, and then choose **Launch Instances**.
5. Choose **View Instances**.