

Amazon Web Services

AWS is a very powerful platform as a service (PaaS) that allows us to serve our applications to the world. In this class we're going to use it to serve group and final projects.

Getting Started

The first thing to do is sign up for an AWS account. Do so by heading to [this link](#) and following the prompts. When you have your account created, you can log into your **root** account [here](#). Once signed in you should see something like the below screenshot.

The screenshot shows the AWS Management Console homepage. The top navigation bar includes the AWS logo, a 'Services' dropdown, 'Resource Groups', and account information for '7FProd' in 'N. Virginia'. Below the navigation is a search bar and a 'Helpful tips' sidebar.

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services:

- EC2
- VPC
- Directory Service
- IAM
- CloudWatch

All services:

- Compute**
 - EC2
 - EC2 Container Service
 - Lightsail
 - Elastic Beanstalk
 - Lambda
 - Batch
- Storage**
 - S3
 - EFS
 - Glacier
 - Storage Gateway
- Database**
 - RDS
 - DynamoDB
 - ElastiCache
 - Amazon Redshift
- Networking & Content Delivery**
 - VPC
 - CloudFront
 - Direct Connect
 - Route 53
- Migration**
 - AWS Migration Hub
- Analytics**

Helpful tips

Manage your costs
Get real-time billing alerts based on your cost and usage budgets. [Start now](#)

Create an organization
Use AWS Organizations for policy-based management of multiple AWS accounts. [Start now](#)

Explore AWS

Amazon Relational Database Service (RDS)
RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. [Learn more](#).

Real-Time Analytics with Amazon Kinesis
Stream and analyze real-time data, so you can get timely insights and react quickly. [Learn more](#).

Get Started with Containers on AWS
Amazon ECS helps you build and scale containers for any size application. [Learn more](#).

AWS Marketplace
Discover, procure, and deploy popular software products that run on AWS. [Learn more](#).

Have feedback?
Submit feedback to tell us about your experience with the AWS Management Console.

Setting up your user

Per AWS best practice you don't want to be logging into your root account to do things. So, we're going to create an IAM user for you to use when using your account. To do so, navigate to the [IAM section](#) of the console. You'll see something like below.

Screenshot of the AWS IAM Management Console dashboard.

The dashboard shows the following information:

- Welcome to Identity and Access Management**
- IAM users sign-in link: <https://7factor.signin.aws.amazon.com/console>
- IAM Resources**
 - Users: 2
 - Groups: 0
 - Customer Managed Policies: 0
 - Roles: 2
 - Identity Providers: 0
- Security Status**: 3 out of 5 complete.
 - Completed**: Delete your root access keys
 - Pending**: Activate MFA on your root account
 - Completed**: Create individual IAM users
 - Pending**: Use groups to assign permissions
 - Completed**: Apply an IAM password policy
- Feature Spotlight**: Introduction to AWS IAM (Video thumbnail)
- Additional Information**: IAM best practices, IAM documentation, Web Identity Federation Playground, Policy Simulator, Videos, IAM release history and additional resources.

Make note of the “IAM User sign in link” and customize it if you want so it’s easier to remember. This is where you’ll go to sign in after we create your IAM user. Click on users, then [new user](#). Fill out your information, and be sure to uncheck “User must create a new password at next sign-in” unless you want to enter a new password.

IAM Management Console

Secure | https://console.aws.amazon.com/iam/home?region=us-east-1#/users\$new?step=details

aws Services Resource Groups

7FProd Global Support

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password
 Custom password

Show password

Require password reset User must create a new password at next sign-in

* Required

[Cancel](#) [Next: Permissions](#)

[Feedback](#) [English \(US\)](#)

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

The next screen dictates what permissions your users gets. AWS IAM permissions is a deep topic with lots options, to keep it simple make the same selections as displayed below.

Screenshot of the AWS IAM Management Console showing the "Set permissions for robot" step. The screen displays three options for granting permissions: "Add user to group", "Copy permissions from existing user", and "Attach existing policies directly". The third option is highlighted. Below this, a list of 280 available policies is shown, with "AdministratorAccess" selected. At the bottom, there are "Cancel", "Previous", and "Next: Review" buttons.

Set permissions for robot

Add user to group Copy permissions from existing user Attach existing policies directly

Attach one or more existing policies directly to the users or create a new policy. [Learn more](#)

[Create policy](#) [Refresh](#)

	Policy name	Type	Attachments	Description
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	1	Provides full access to AWS services and resources.
<input type="checkbox"/>	AmazonAPIGatewayAdmin...	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gat...
<input type="checkbox"/>	AmazonAPIGatewayInvoke...	AWS managed	0	Provides full access to invoke APIs in Amazon API Gateway.
<input type="checkbox"/>	AmazonAPIGatewayPushT...	AWS managed	0	Allows API Gateway to push logs to user's account.
<input type="checkbox"/>	AmazonAppStreamFullAcc...	AWS managed	0	Provides full access to Amazon AppStream via the AWS Manage...
<input type="checkbox"/>	AmazonAppStreamReadO...	AWS managed	0	Provides read only access to Amazon AppStream via the AWS M...
<input type="checkbox"/>	AmazonAppStreamService...	AWS managed	0	Default policy for Amazon AppStream service role.
<input type="checkbox"/>	AmazonAthenaFullAccess	AWS managed	0	Provide full access to Amazon Athena and scoped access to the ...
<input type="checkbox"/>	AmazonChimeFullAccess	AWS managed	0	Provides full access to Amazon Chime Admin Console via the A...
<input type="checkbox"/>	AmazonChimeReadOnly	AWS managed	0	Provides read only access to Amazon Chime Admin Console via t...

Showing 280 results

Cancel Previous **Next: Review**

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

On the review screen double check to make sure everything looks good and then click “Create user”. You’ll see another screen:

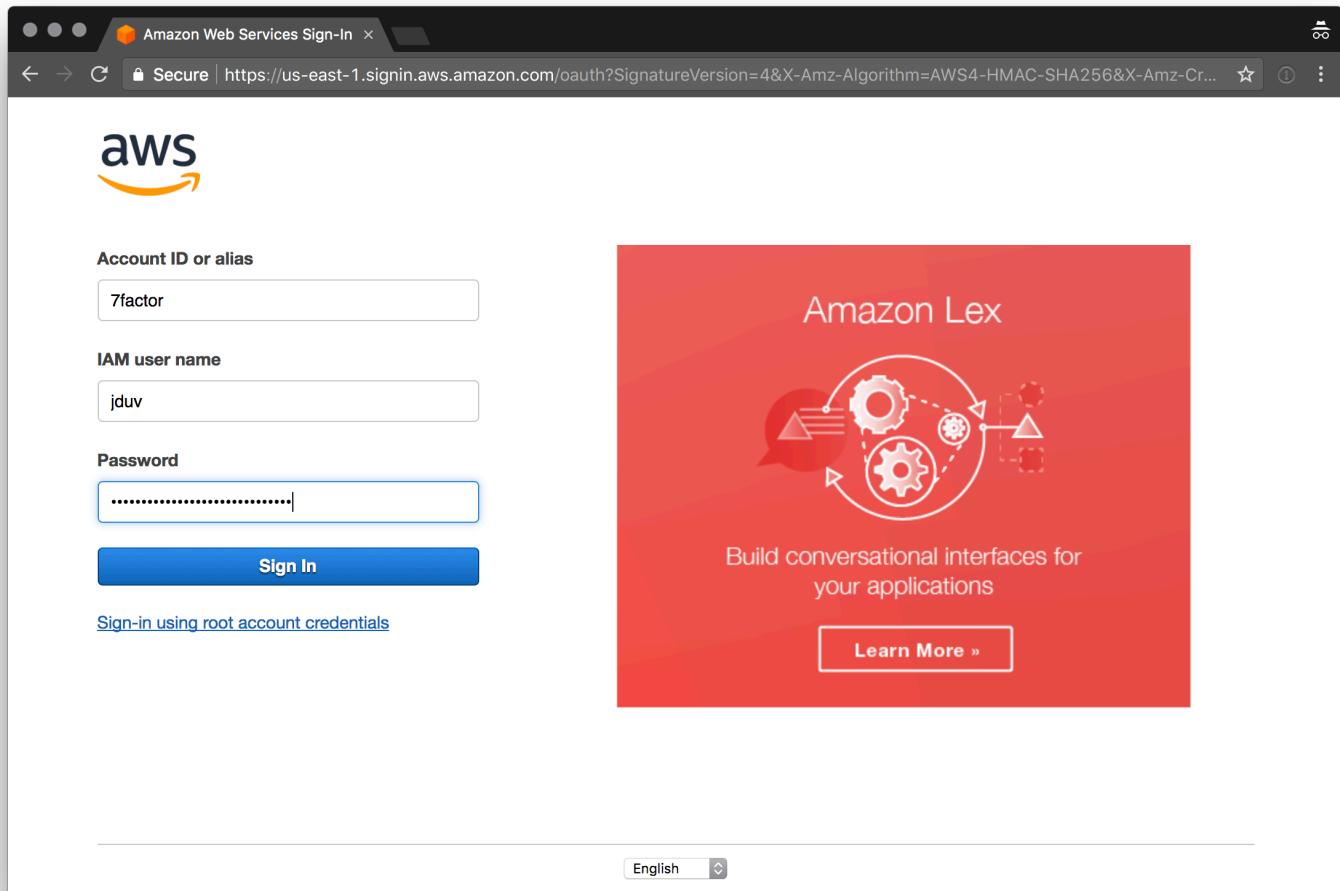
The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home?region=us-east-1#/users\\$new?step=final&accessKey&login&userNames=robot&passwordT...](https://console.aws.amazon.com/iam/home?region=us-east-1#/users$new?step=final&accessKey&login&userNames=robot&passwordT...). The page title is "Add user". A progress bar at the top indicates four steps: 1. Details (grey), 2. Permissions (grey), 3. Review (grey), and 4. Complete (blue). A green success message box contains the text: "Success: You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time." Below the message, it says "Users with AWS Management Console access can sign-in at: <https://7factor.signin.aws.amazon.com/console>". There is a "Download .csv" button. A table displays user information:

	User	Access key ID	Secret access key	Password	Email login instructions
▶	robot	AKIAIYFPRE5YJ5NCFSYQ	***** Show	***** Show	Send email

At the bottom, there are links for "Feedback", "English (US)", and "Close".

This screen contains three **very important** pieces of information. First, the password you will be using to log into the console as a non-root user. You set this earlier, so it shouldn't change. Next, this screen displays your AWS secret key and access key. Save these values in a very safe location, and **never ever check them into source control or make them public to anyone**. We're not responsible for your \$10k AWS bill if you do so.

Now, let's head over to the “IAM Sign in link” you noted earlier. Your account ID should be filled in.



Hooray! You're done! A couple of things to remember:

1. When you create any resource in AWS you will immediately begin paying for it. AWS charges you on a per minute basis for billable elements.
2. Never ever ever ever check your access codes into a repository that is public. You will regret it.
3. Try to do everything from the IAM user instead of the root console (i.e. logging in with your email address). IAM users allow you to protect aspects of your environment—and when you become more proficient at using them they're pretty neat.

The Default VPC

AWS segregates computing resources into constructs called Virtual Private Clouds, or VPCs. Every account comes with a default VPC. Inside there, we can place compute resources (and many other cool things) to run our stuff on. Navigate to the [VPC section](#) of your console. You should see something like this:

The screenshot shows the AWS VPC Management Console dashboard. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, 'Resource Groups' dropdown, and user information ('jduv @ 7factor', 'N. Virginia', 'Support'). Below the navigation is a search bar with the URL 'https://console.aws.amazon.com/vpc/home?region=us-east-1#'. The main content area has a left sidebar titled 'Virtual Private Cloud' with links for 'Your VPCs', 'Subnets', 'Route Tables', 'Internet Gateways', 'Egress Only Internet Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Endpoints', 'NAT Gateways', 'Peering Connections', 'Security', and 'Network ACLs'. The main panel is titled 'Resources' and contains two buttons: 'Start VPC Wizard' (blue) and 'Launch EC2 Instances' (grey). A note says 'Note: Your Instances will launch in the US East (N. Virginia) region.' Below this, it says 'You are using the following Amazon VPC resources in the US East (N. Virginia) region:' followed by a table of resource counts:

2 VPCs	2 Internet Gateways
0 Egress-only Internet Gateways	3 Subnets
3 Route Tables	2 Network ACLs
0 Elastic IPs	0 VPC Peering Connections
0 Endpoints	0 Nat Gateways
8 Security Groups	5 Running Instances
0 VPN Connections	0 Virtual Private Gateways
0 Customer Gateways	

Below the resources, there's a section titled 'VPN Connections' with a note: 'Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.' At the bottom of the main panel are 'Create VPN Connection' and 'Feedback' buttons.

Your environment will be much less busy than the example above. Click on the [VPCs link](#). You'll be greeted with a list of all the VPCs in your environment. Click on your default VPC (the only one in the list) and you'll see something like below.

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar titled "Virtual Private Cloud" with various options like "Your VPCs", "Subnets", "Route Tables", etc. The main area shows a table of VPCs with columns for Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, and DHCP options set. One VPC, "main-vpc" (ID: vpc-87f5a6e0), is selected and shown in more detail. The "Summary" tab is active, displaying information such as VPC ID, State, CIDR blocks, Network ACL, Tenancy, DNS resolution, and DHCP options set. Below the summary, there are tabs for "CIDR Blocks", "Flow Logs", and "Tags". At the bottom of the page, there are links for "Feedback", "English (US)", and legal notices.

As you can tell, VPCs are pretty complex. You should take note of is the funny little thing called a **CIDR** block. This is a template for the **IP addresses** that all of the resources placed in this VPC will get. So, in the example above you can count on any virtual machine we create will have the IP address of 172.31.X.Y where X and Y can be any number from 0 to 255.

DNS resolution

Ensure that in your VPC's settings you have values set to "yes" for **DNS Hostnames** and **DNS Resolution**. If they're not, edit them using the drop down menu as displayed below.

The screenshot shows the AWS VPC Management Console. On the left, there's a sidebar with various VPC-related options like Subnets, Route Tables, and Internet Gateways. The main area displays a table of VPCs with one row selected. A context menu is open over this row, listing actions: Delete VPC, Edit CIDRs, Create Default VPC, Edit DHCP Options Set, **Edit DNS Resolution**, Edit DNS Hostnames, and Create Flow Log. Below the table, a detailed view for the selected VPC (vpc-87f5a6e0 | main-vpc) is shown with tabs for Summary, CIDR Blocks, Flow Logs, and Tags. The Summary tab lists VPC details: VPC ID: vpc-87f5a6e0 | main-vpc, State: available, IPv4 CIDR: 172.31.0.0/16, IPv6 CIDR: (empty), DHCP options set: dopt-4df58e29, Route table: rtb-15c77073. It also shows Network ACL: acl-172f2170, Tenancy: Default, DNS resolution: yes, DNS hostnames: yes, and ClassicLink DNS Support: no.

Creating an EC2 Instance

Navigate to the [EC2 instance](#) section of your environment. You'll see a screen similar to the VPC screen.

The screenshot shows the AWS EC2 Management Console dashboard for the US East (N. Virginia) region. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (with sub-links for Instances, Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts), Images (with sub-links for AMIs, Bundle Tasks), Elastic Block Store (with sub-links for Volumes, Snapshots), Network & Security (with sub-links for Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and Load Balancing (with sub-link for Load Balancers). The main content area displays resource counts: 4 Running Instances, 0 Dedicated Hosts, 7 Volumes, 2 Key Pairs, 0 Placement Groups, 0 Elastic IPs, 0 Snapshots, 1 Load Balancers, and 6 Security Groups. A callout box suggests trying Amazon Lightsail for free. Below this, there's a 'Create Instance' section with a 'Launch Instance' button, a note about launching in the US East (N. Virginia) region, and sections for Service Health and Scheduled Events. The Service Status for US East (N. Virginia) shows 'No events' and 'This service is operating normally'. The Scheduled Events section shows 'No events'. The right sidebar includes links for Account Attributes (Supported Platforms: VPC, Default VPC vpc-87f5a6e0, Resource ID length management), Additional Information (Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, Contact Us), and an AWS Marketplace section featuring Barracuda NextGen Firewall F-Series - PAYG, provided by Barracuda Networks, Inc., with a 5-star rating.

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Spot Requests

Reserved Instances

Scheduled Instances

Dedicated Hosts

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

LOAD BALANCING

Load Balancers

Feedback

English (US)

Secure | https://console.aws.amazon.com/ec2/v2/home?region=us-east-1

Services ▾ Resource Groups ▾

jduv @ 7factor ▾ N. Virginia ▾ Support ▾

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) region:

4 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
7 Volumes	1 Load Balancers
2 Key Pairs	6 Security Groups
0 Placement Groups	

Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free.

Create Instance

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

Launch Instance

Note: Your instances will launch in the US East (N. Virginia) region

Service Health

Service Status:

US East (N. Virginia): This service is operating normally

Availability Zone Status:

Scheduled Events

US East (N. Virginia): No events

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Account Attributes

Supported Platforms

VPC

Default VPC

vpc-87f5a6e0

Resource ID length management

Additional Information

Getting Started Guide

Documentation

All EC2 Resources

Forums

Pricing

Contact Us

AWS Marketplace

Find free software trial products in the AWS Marketplace from the [EC2 Launch Wizard](#). Or try these popular AMIs:

Barracuda NextGen Firewall F-Series - PAYG

Provided by Barracuda Networks, Inc.

Rating ★★★★☆

Click on instances. Your environment will be pretty bare, but if you had some resources it might look like below.

The screenshot shows the AWS EC2 Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (which is selected), Spot Requests, Reserved Instances, Scheduled Instances, Dedicated Hosts, Images (AMIs), Bundle Tasks, Elastic Block Store (Volumes, Snapshots), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces). The main content area displays a table of running instances:

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Stat
<input type="checkbox"/>	concourse-w...	i-055b377b2d3bc9dda	t2.small	us-east-1e	running	2/2 checks ...	None
<input type="checkbox"/>	concourse-web	i-05dc8348ea162c13b	t2.medium	us-east-1e	running	2/2 checks ...	None
<input type="checkbox"/>	concourse-p...	i-0ad6d41934284a8...	t2.micro	us-east-1e	running	2/2 checks ...	None
<input type="checkbox"/>		i-0bb5770dc092acb3f	t2.micro	us-east-1b	terminated		None
<input type="checkbox"/>	concourse-w...	i-0cab465270225f164	t2.small	us-east-1e	running	2/2 checks ...	None

Below the table, a message says "Select an instance above". At the bottom of the page are links for Feedback, English (US), Copyright notice (2008-2017), Privacy Policy, and Terms of Use.

To create a new instance, click launch instance. You'll be greeted with a fairly complicated flow. Let's walk through it.

On the first screen we're choosing the operating system for our instance. For the purposes of this class, please use Ubuntu Server (free tier eligible).

EC2 Management Console

Secure | https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Free tier only (i)

Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-6057e21a

Select

Amazon Linux Free tier eligible

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Red Hat Enterprise Linux 7.4 (HVM), SSD Volume Type - ami-c998b6b2

Select

Red Hat Free tier eligible

Red Hat Enterprise Linux version 7.4 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type - ami-3943f043

Select

SUSE Linux Free tier eligible

SUSE Linux Enterprise Server 12 Service Pack 3 (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

Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-da05a4a0

Select

Ubuntu Server 16.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from

Feedback English (US)

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

K < 1 to 35 of 35 AMIs >|

64-bit

64-bit

64-bit

64-bit

Next we're picking the hardware configuration of the instance. Pick **t2.micro** since it's free for up to 60 hours of compute time per month.

The screenshot shows the AWS EC2 Management Console interface for launching a new instance. The top navigation bar includes the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, and user information ('jduv @ 7factor', 'N. Virginia', 'Support'). Below the navigation is a progress bar with steps: '1. Choose AMI', '2. Choose Instance Type' (which is underlined in orange), '3. Configure Instance', '4. Add Storage', '5. Add Tags', '6. Configure Security Group', and '7. Review'. A 'Filter by:' dropdown set to 'All instance types' and a 'Current generation' dropdown are visible. A note at the top says 'Step 2: Choose an Instance Type' and describes the variety of instance types available. The main content area displays a table of instance types:

	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 checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input 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

At the bottom of the screen are buttons for 'Cancel', 'Previous', 'Review and Launch' (which is highlighted in blue), and 'Next: Configure Instance Details'.

The next screen describes how many and where the instances will be placed with respect to your VPC. You should be able to leave everything as it's default.

The screenshot shows the AWS EC2 Management Console Launch Instance Wizard at Step 3: Configure Instance Details. The page title is "Step 3: Configure Instance Details". Below it, a sub-instruction reads: "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." The configuration form includes the following fields:

- Number of instances:** 1 (with a "Launch into Auto Scaling Group" link)
- Purchasing option:** Request Spot instances
- Network:** vpc-87f5a6e0 | main-vpc (default) (with a "Create new VPC" link)
- Subnet:** subnet-4c26a328 | build-net-1a | us-east-1a (with a "Create new subnet" link)
251 IP Addresses available
- Auto-assign Public IP:** Use subnet setting (Disable)
- IAM role:** None (with a "Create new IAM role" link)
- 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.

A collapsed section titled "▼ Network interfaces" is shown. At the bottom of the page are navigation buttons: Cancel, Previous, Review and Launch (highlighted in blue), and Next: Add Storage.

Now click “Review and Launch.” The other settings should be good with respect to their defaults. We will revisit the concept of security groups later. Scroll through the settings and click a final “launch” which will display the following:

Step 7: Review Instance Launch

Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-6057e21a

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java.

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

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

Name your key pair, click “download key pair” and save the PEM file in a very safe place. If you lose it you will not be able to access your EC2 instance ever again.

You’re done! If you check your EC2 dashboard you should see the instance spinning up. Once it’s available you will be able to access it using SSH.