

## Introduction

A Launch Template is a template that an Auto Scaling group uses to launch Amazon EC2 instances. If you've launched an individual EC2 instance before, you've already walked through the process of defining compute characteristics such as the instance type, security groups, and configuration scripts. A launch template allows you to define these same characteristics, which are then applied to any instances launched in the Auto Scaling group that references the Launch Template. The Launch Template essentially contains the blueprint or DNA for the exact type of instance that should be launched. Hence, when auto-scaling, each instance is guaranteed to be just like the last one. It's repeatable, scalable, and reliable.

When you create the Launch Template you will include information such as the Amazon machine image ID (AMI) to use for launching the EC2 instance, the instance type, key pairs, security groups, and block device mappings, among other configuration settings. When you create your Auto Scaling group, you must associate it with a Launch Template.

First, you will create a security group for your instances, then you will create a Launch Template.

## Instructions

1. [Navigate to EC2 in the AWS Management Console.](#)
2. In the left-hand menu, under **Network & Security**, click **Security Groups**:



3. To start creating a new security group, click **Create security group**:

Create security group

4. Under **Basic details**, in the **Security group name** field, enter *webserver-cluster*:

Security group name

webserver-cluster

5. In the **Description** field, enter *Webserver security group*:

Description **Info**

Webserver security group

6. In the **Inbound rules** section, click **Add rule**:

New fields allowing you to specify a rule will appear.

7. To configure a rule allowing SSH traffic, enter the following values:

- **Type:** Enter *SSH* and select **SSH**
- **Source:** Select **Anywhere-IPv4**
- **Description:** Enter *SSH*

SSH ▼	TCP	22	Anywh... ▼	Q	SSH
				0.0.0.0/0 ✕	

You have added this rule so that later you can access instances using SSH.

8. To add another inbound rule, click **Add rule** again in the **Inbound rules** section.

9. To configure a rule allowing HTTP traffic, enter the following values:

- **Type:** Enter *HTTP* and select **HTTP**
- **Source:** Select **Anywhere-IPv4**
- **Description:** Enter *HTTP*

HTTP ▼	TCP	80	Anywh... ▼	Q	HTTP
				0.0.0.0/0 ✕	

You have added two inbound rules.

In this lab, you are allowing access from anywhere (**0.0.0.0/0**). In a non-lab environment, you are likely to be required to have a much more restrictive **Source**. For example, you may be required to specify a corporate IP range to reduce the likelihood of unauthorized access.

10. To finish creating your security group, scroll to the bottom of the page and click **Create security group**:

An orange rectangular button with the text "Create security group" in white.

You will see a notification that your security group has been created:

A green rectangular notification box with a white checkmark icon on the left. The text inside reads: "Security group (sg-00e9efbbc41be7906 | Webserver-cluster) was created successfully".

✔ Security group (sg-00e9efbbc41be7906 | Webserver-cluster) was created successfully

▶ Details

You have created a security group that you can specify in the launch template you are about to create.

11. In the left-hand menu, under **Instances**, click **Launch Templates**:

A light orange rectangular button with the text "Launch Templates" in a darker orange color.

12. To open the **Launch Templates** page and click the **Create launch template** button:

An orange rectangular button with the text "Create launch template" in white.

The create launch template form will load.

13. In the **Launch template name and description** section, enter the following values accepting the defaults for fields not specified:

- **Launch template name:** *webserver-cluster*

- **Template version description:** *Lab launch template*
- **Provide guidance to help me set up a template that I can use with EC2 Auto Scaling:** *checked* (this setting makes some fields required)

Launch template name - *required*

webserver-cluster

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '

Template version description

Lab launch template

Max 255 chars

Auto Scaling guidance [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

- ☒ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling


14. Scroll down to the **Application and OS Images (Amazon machine Image)** section, select the **Amazon Linux** box:

## ▼ Application and OS Images (Amazon machine Image) - required [Info](#)


An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

 Search our full catalog including 1000s of application and OS images


### Quick Start




Amazon Linux



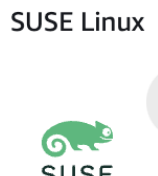
Ubuntu




Windows



Red Hat



SUSE Linux



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

### Amazon Machine Image (AMI)

**Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type**  
ami-066333d9c572b0680 (64-bit (x86)) / ami-0deb314c20acdd478 (64-bit (Arm))  
Virtualization: hvm    ENA enabled: true    Root device type: ebs

Free tier eligible ▼

### Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20211223.0 x86\_64 HVM gp2

### Architecture

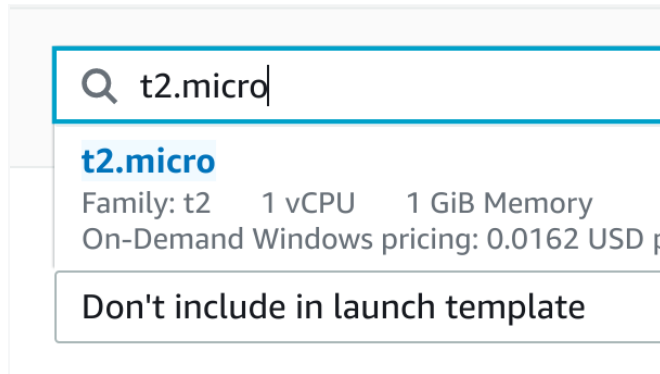
### AMI ID

64-bit (x86) ▼

ami-066333d9c572b0680

**Note:** Ensure that the AMI for the **64-bit (x86)** architecture is selected.

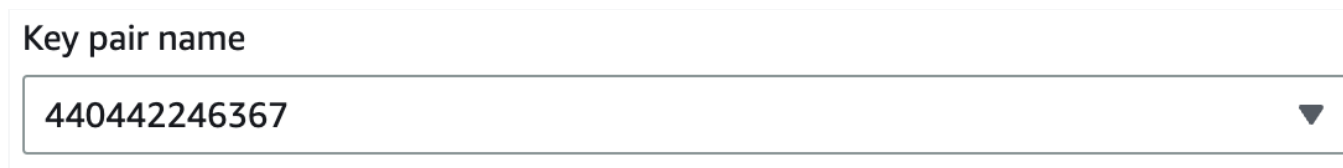
15. In the **Instance type** field, enter *t2.micro* and click the **t2.micro** result:



The screenshot shows a search bar with the text 't2.micro' entered. Below the search bar, the results for 't2.micro' are displayed. The first result is 't2.micro' in blue text. Below it, the details are listed: 'Family: t2', '1 vCPU', '1 GiB Memory', and 'On-Demand Windows pricing: 0.0162 USD p'. At the bottom of the results, there is a button that says 'Don't include in launch template'.

Be aware that in this lab you are restricted from using larger instances, trying to launch other types of instance may result in your CloudAcademy account being temporarily banned.

16. In the **Key pair (login)** section, under **Key pair name**, select the numeric option:

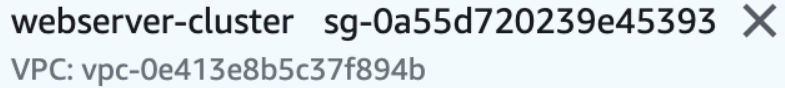


The screenshot shows a dropdown menu labeled 'Key pair name'. The dropdown is open, showing a list of options. The first option is '440442246367', which is highlighted. A downward arrow is visible on the right side of the dropdown menu.

You will use the key pair to access EC2 instances launched with this configuration later in the lab.

In situations where you don't need SSH, you don't have to configure a key pair, this is often preferred in terms of security.

17. Under the **Network Settings** section, click the **Security groups** drop-down and select **webserver-cluster**:



This is the security group you created earlier.

Notice that you have created separate security groups for the instances and the load balancer. In a non-lab environment, it is often the case that the instances are listening on a different port than the load balancer, and the load balancer re-directs the traffic. Assigning separate security groups allows you to more flexibly control and restrict traffic at the network level.

18. Take a look at the **Storage (volumes)** section.

This part of the form allows you to add or increment the size of any EBS volume attached to each EC2 instance started by the Auto Scaling group. Leave the defaults and do not add any EBS volumes.

Typically large EBS volumes are only needed if your software requires storage space to process the application data. Many applications store raw or processed data with Amazon S3, Redshift, DynamoDB, or another storage/database service provided by Amazon. When that is the use case, large EBS volumes are usually not required. This lab environment does not need extra disk space.

19. Scroll down to the bottom and click **Advanced details**:



More configuration options will appear.



20. Scroll down to the **Detailed CloudWatch monitoring** option, and click **Enable**:

Detailed CloudWatch monitoring

Enable

By default, CloudWatch monitors EC2 instances approximately every 5 minutes. Detailed monitoring enables monitoring more often (each minute).

*Note:* Enabling detailed monitoring incurs an extra cost.

21. In the **User data** text-box at the bottom of the page, enter the following script:



```
1  #!/bin/bash
2  # Enable the epel-release
3  sudo amazon-linux-extras install epel
4  # Install and start Apache web server
5  sudo yum install -y httpd php
6  # Start the httpd service
7  service httpd start
8  # Install CPU stress test tool
9  sudo yum install -y stress
```

This bash script installs PHP, an Apache webserver (httpd), and a tool for stress testing called Stress.

*Warning:* The EC2 instances will never reach 100% CPU Utilization due to the limitations of the burstable credit. They should reach an usage of about **80%**.

22. To create your Launch Template, click **Create launch template**:

**Create launch template**

You will see a notification that your launch template has been created:



**Success**

Successfully created [webserver-cluster \(lt-005b3f6441207c3c2\)](#)

► **Actions log**

24. To return to the EC2 management console, click **View launch templates**:

**View launch templates**

## Summary

You have created a security group and you created a launch template that can be used by an auto-scaling group to launch identical instances every time.

VALIDATION CHECKS

## 1 Checks

Check again 



### Created Launch Template

Check if the launch template has been created

Amazon EC2