Assignment-16-May-2022

1. What is a launch template?

* A launch template provides full functionality for Amazon EC2 Auto Scaling
* It reduces the number of steps that are required to create an AWS instance by capturing all launch parameters within one resource.
* Also, newer features of Amazon EC2 such as the current generation of Amazon EBS

(a) Provisioned IOPS volumes (io2)

(b) EBS volume tagging

(c) T2 Unlimited instances

(d) Elastic Inference

(e) Dedicated Hosts.

1. Hands on- Create Launch Template?

: **To create a launch template**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. On the navigation pane, under **Instances**, choose **Launch Templates**.
3. Choose **Create launch template**. Enter a name and provide a description for the initial version of the launch template.
4. Under **Auto Scaling guidance**, select the check box to have Amazon EC2 provide guidance to help create a template to use with Amazon EC2 Auto Scaling.
5. Under **Launch template contents**, fill out each required field and any optional fields as needed.
   1. **Application and OS Images (Amazon Machine Image)**: (Required) Choose the ID of the AMI for your instances.

You can search through all available AMIs, or select an AMI from the **Recents** or **Quick Start** list. If you don't see the AMI that you need, choose **Browse more AMIs** to browse the full AMI catalog.

To choose a custom AMI, you must first create your AMI from a customized instance.

For more information, see [Create an AMI](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-ami.html) in the Amazon EC2 User Guide for Linux Instances.

* 1. For **Instance type**, choose a single instance type that's compatible with the AMI that you specified.

Alternatively, to launch an Auto Scaling group with multiple instance types, choose **Advanced**, **Specify instance type attributes**, and then specify the following options:

* + - **Number of vCPUs**: Enter the minimum and maximum number of vCPUs. To indicate no limits, enter a minimum of 0, and keep the maximum blank.
    - **Amount of memory (MiB)**: Enter the minimum and maximum amount of memory, in MiB. To indicate no limits, enter a minimum of 0, and keep the maximum blank.
    - Expand **Optional instance type attributes** and choose **Add attribute** to further limit the types of instances that can be used to fulfill your desired capacity. For information about each attribute, see [InstanceRequirementsRequest](https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_InstanceRequirementsRequest.html) in the Amazon EC2 API Reference.
    - **Resulting instance types**: You can view the instance types that match the specified compute requirements, such as vCPUs, memory, and storage.
    - To exclude instance types, choose **Add attribute**. From the **Attribute** list, choose **Excluded instance types**. From the **Attribute value** list, select the instance types to exclude.

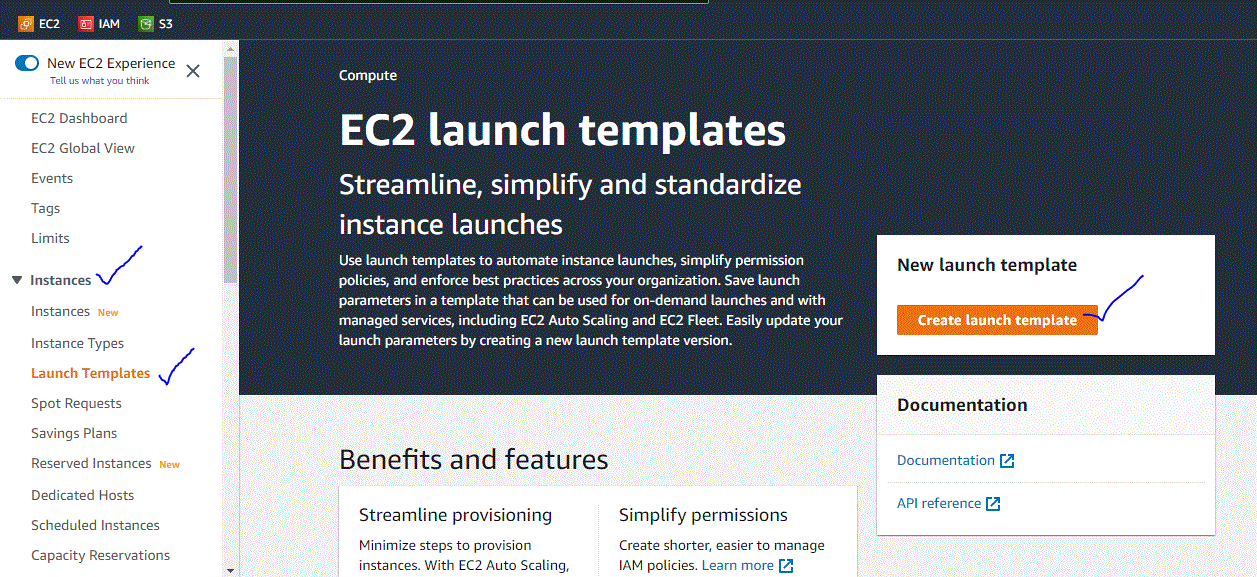
For more information, see [Create an Auto Scaling group using attribute-based instance type selection](https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-asg-instance-type-requirements.html).

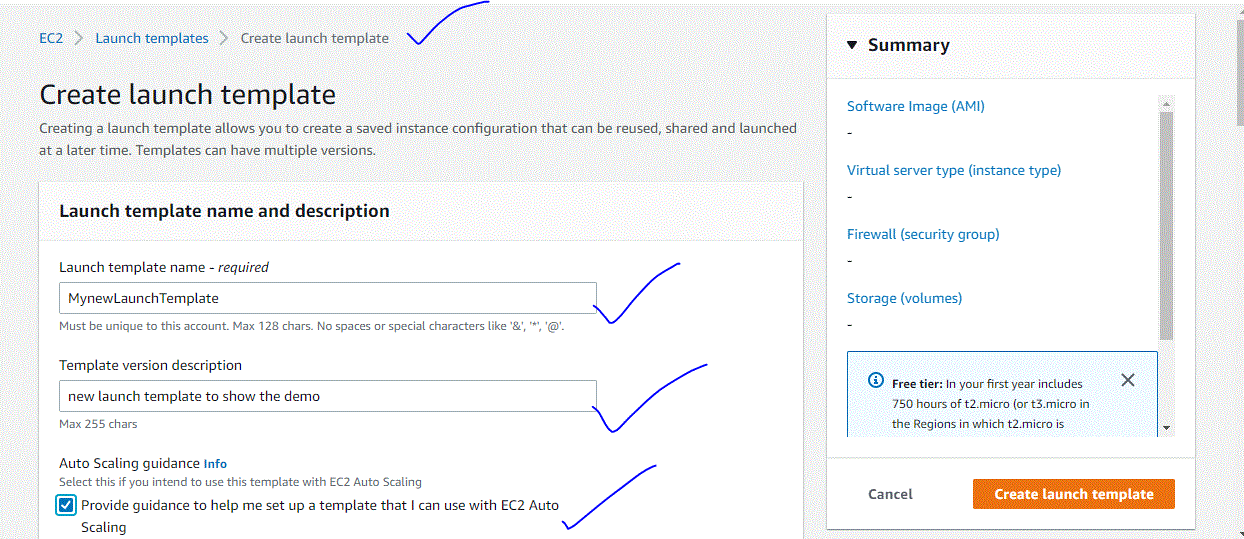
* 1. **Key pair (login)**: For **Key pair name**, choose an existing key pair, or choose **Create new key pair** to create a new one. For more information, see [Amazon EC2 key pairs and Linux instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html) in the Amazon EC2 User Guide for Linux Instances.
  2. **Network settings**: For **Firewall (security groups)**, use one or more security groups, or keep this blank and configure one or more security groups as part of the network interface. For more information, see [Amazon EC2 security groups for Linux instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html) in the Amazon EC2 User Guide for Linux Instances.

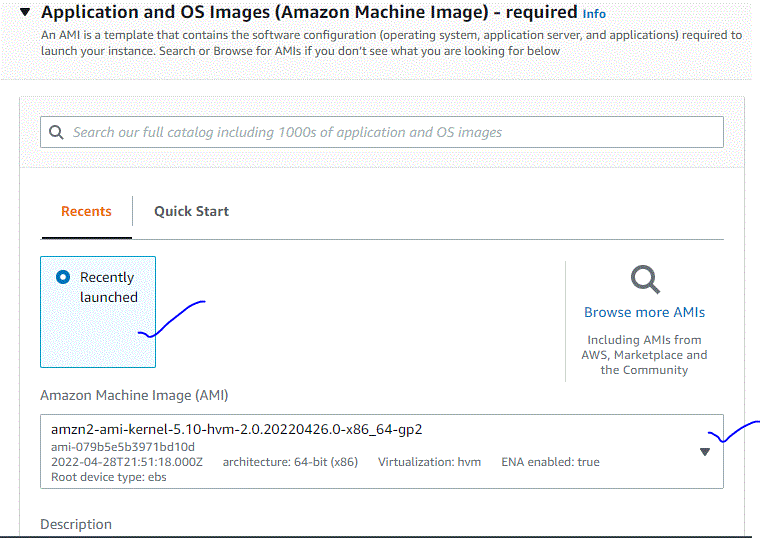
If you don't specify any security groups in your launch template, Amazon EC2 uses the default security group for the VPC that your Auto Scaling group will launch instances into. By default, this security group doesn't allow inbound traffic from external networks. For more information, see [Default security groups for your VPCs](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#DefaultSecurityGroup) in the Amazon VPC User Guide.

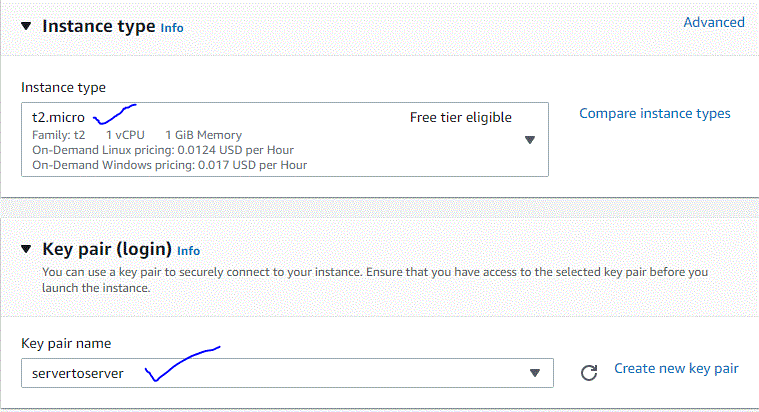
* 1. Do one of the following:
     + Change the default network interface settings. For example, you can enable or disable the public IPv4 addressing feature, which overrides the auto-assign public IPv4 addresses setting on the subnet. For more information, see [Change the default network interface settings](https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-launch-template.html#change-network-interface).
     + Skip this step to keep the default network interface settings.
  2. Do one of the following:
     + Modify the storage configuration. For more information, see [Modify the storage configuration](https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-launch-template.html#modify-storage-configuration).
     + Skip this step to keep the default storage configuration.
  3. For **Resource tags**, specify tags by providing key and value combinations. If you specify instance tags in your launch template and then you choose to propagate your Auto Scaling group's tags to its instances, all the tags are merged. If the same tag key is specified for a tag in your launch template and a tag in your Auto Scaling group, then the tag value from the group takes precedence.

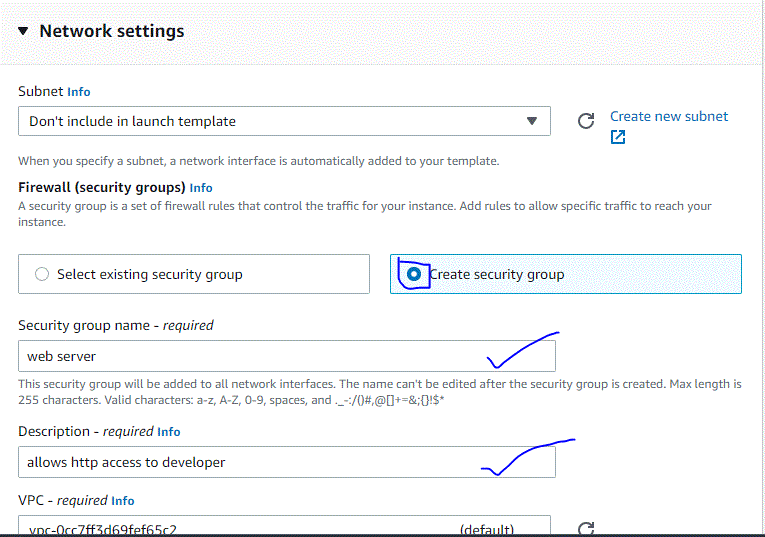
1. (Optional) Configure advanced settings. For more information, see [Configure advanced settings for your launch template](https://docs.aws.amazon.com/autoscaling/ec2/userguide/create-launch-template.html#advanced-settings-for-your-launch-template).
2. When you are ready to create the launch template, choose **Create launch template**.
3. To create an Auto Scaling group, choose **Create Auto Scaling group** from the confirmation page.

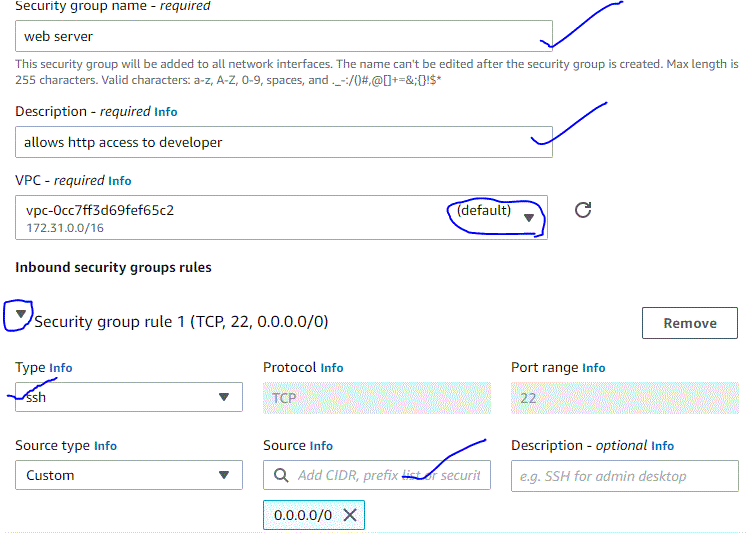


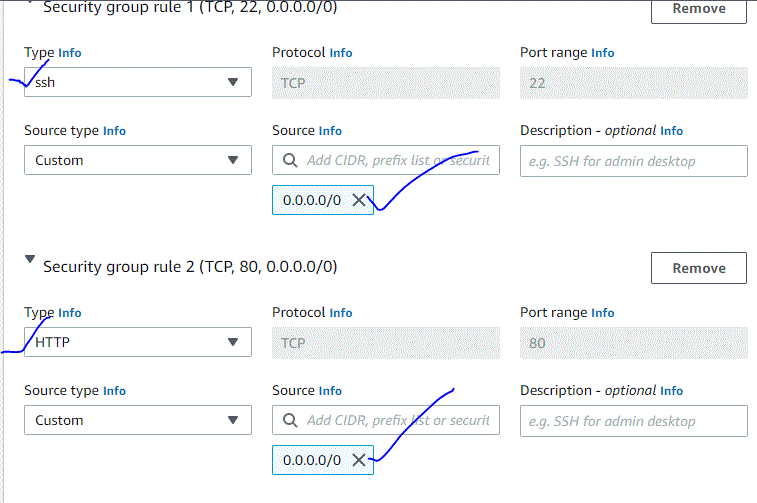


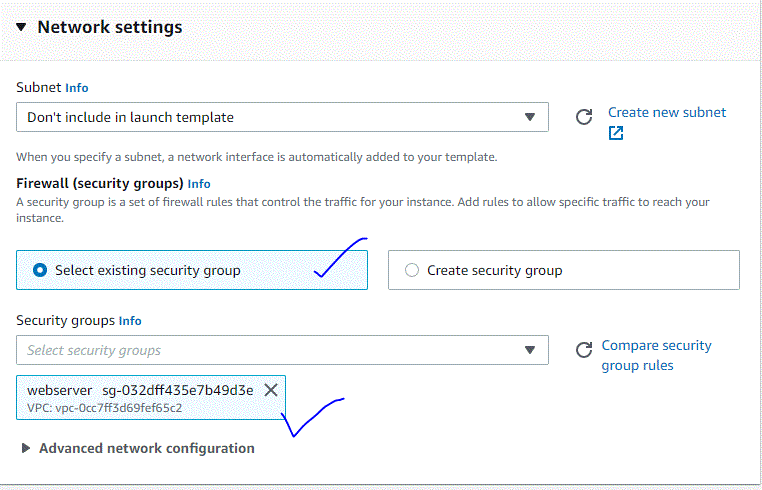




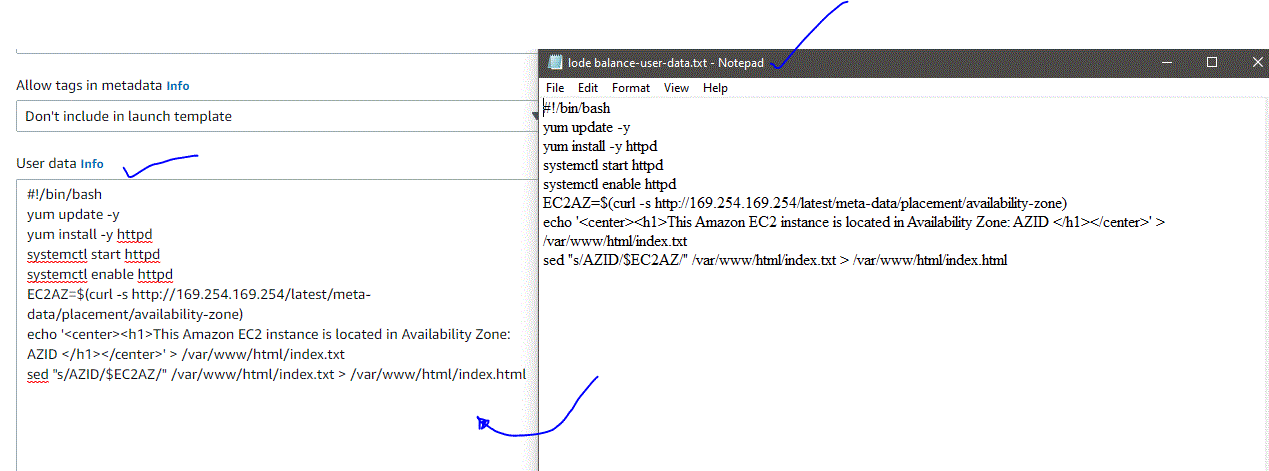




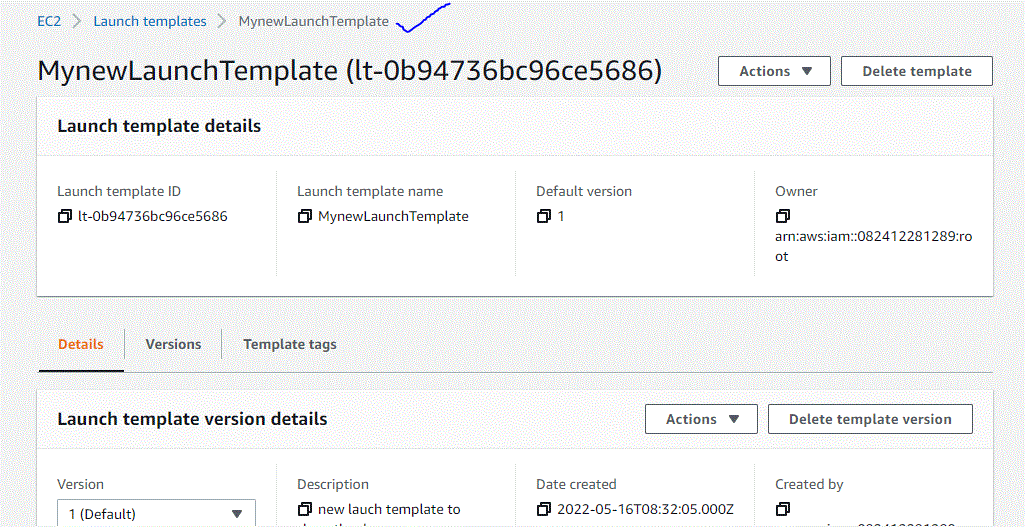












1. Hands on – Create Auto Scaling Group?

: **To create an Auto Scaling group using a launch template (console)**

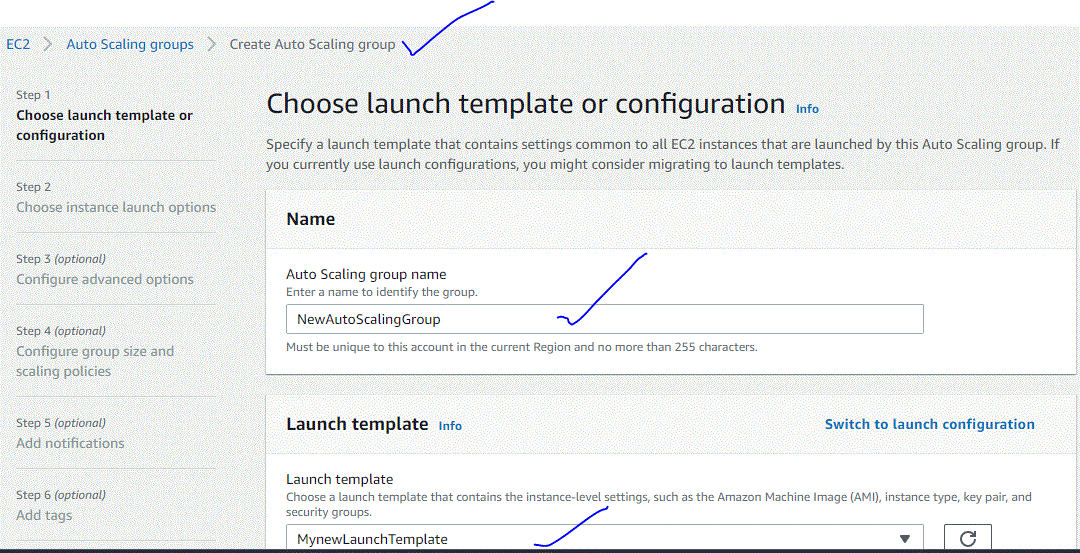
1. Open the Amazon EC2 Auto Scaling console at <https://console.aws.amazon.com/ec2autoscaling/>.
2. On the navigation bar at the top of the screen, choose the same AWS Region that you used when you created the launch template.
3. Choose **Create an Auto Scaling group**.
4. On the **Choose launch template or configuration** page, do the following:
   1. For **Auto Scaling group name**, enter a name for your Auto Scaling group.
   2. For **Launch template**, choose an existing launch template.
   3. For **Launch template version**, choose whether the Auto Scaling group uses the default, the latest, or a specific version of the launch template when scaling out.
   4. Verify that your launch template supports all of the options that you are planning to use, and then choose **Next**.
5. On the **Choose instance launch options** page, under **Network**, for **VPC**, choose a VPC. The Auto Scaling group must be created in the same VPC as the security group you specified in your launch template.
6. For **Availability Zones and subnets**, choose one or more subnets in the specified VPC. Use subnets in multiple Availability Zones for high availability. For more information, see [Considerations when choosing VPC subnets](https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-in-vpc.html#as-vpc-considerations).
7. If you created a launch template with an instance type specified, then you can continue to the next step to create an Auto Scaling group that uses the instance type in the launch template.

Alternatively, you can choose the **Override launch template** option if no instance type is specified in your launch template or if you want to use multiple instance types for auto scaling. For more information, see [Auto Scaling groups with multiple instance types and purchase options](https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-mixed-instances-groups.html).

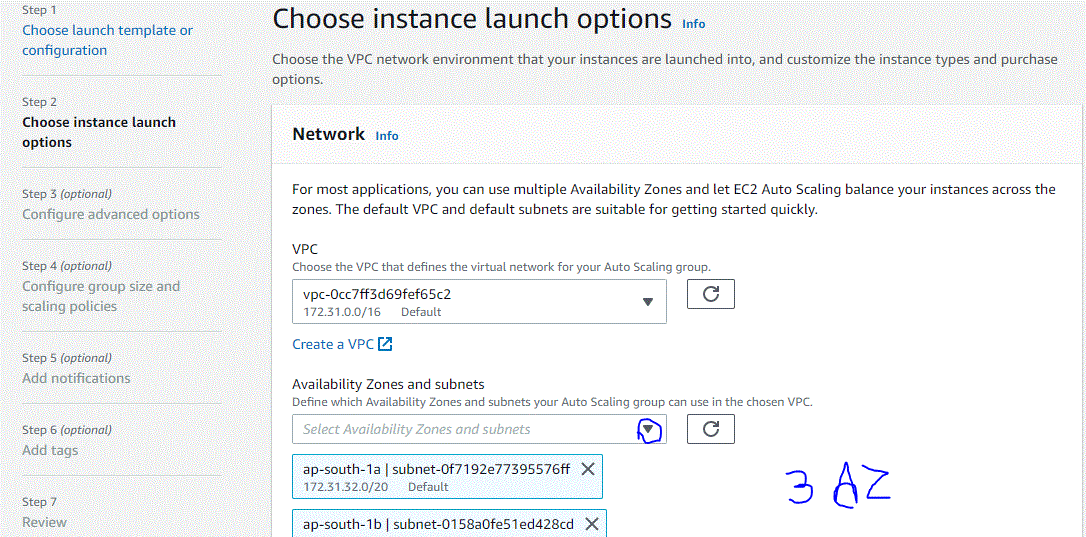
1. Choose **Next** to continue to the next step.

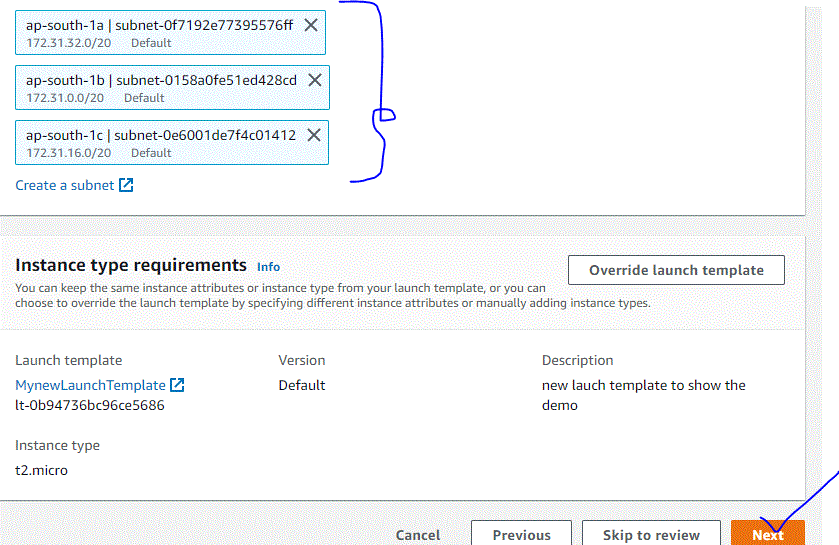
Or, you can accept the rest of the defaults, and choose **Skip to review**.

1. (Optional) On the **Configure advanced options** page, configure the following options, and then choose **Next**:
   1. To register your Amazon EC2 instances with a load balancer, choose an existing load balancer or create a new one. For more information, see [Use Elastic Load Balancing to distribute traffic across the instances in your Auto Scaling group](https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html). To create a new load balancer, follow the procedure in [Configure an Application Load Balancer or Network Load Balancer from the Amazon EC2 Auto Scaling console](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-create-load-balancer-console.html).
   2. To enable your Elastic Load Balancing (ELB) health checks, for **Health checks**, choose **ELB** under **Health check type**. These health checks are optional when you enable load balancing.
   3. Under **Health check grace period**, enter the amount of time until Amazon EC2 Auto Scaling checks the Elastic Load Balancing health status of an instance after it enters the InService state. For more information, see [Health check grace period](https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-health-checks.html#health-check-grace-period).
   4. Under **Additional settings**, **Monitoring**, choose whether to enable CloudWatch group metrics collection. These metrics provide measurements that can be indicators of a potential issue, such as number of terminating instances or number of pending instances. For more information, see [Monitor CloudWatch metrics for your Auto Scaling groups and instances](https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-cloudwatch-monitoring.html).
   5. For **Enable default instance warmup**, select this option and choose the warm-up time for your application. If you are creating an Auto Scaling group that has a scaling policy, the default instance warmup feature improves the Amazon CloudWatch metrics used for dynamic scaling. For more information, see [Set the default instance warmup for an Auto Scaling group](https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-default-instance-warmup.html).
2. (Optional) On the **Configure group size and scaling policies** page, configure the following options, and then choose **Next**:
   1. For **Desired capacity**, enter the initial number of instances to launch. When you change this number to a value outside of the minimum or maximum capacity limits, you must update the values of **Minimum capacity** or **Maximum capacity**. For more information, see [Set capacity limits on your Auto Scaling group](https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-capacity-limits.html).
   2. To automatically scale the size of the Auto Scaling group, choose **Target tracking scaling policy** and follow the directions. For more information, see [Target Tracking Scaling Policies](https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html#policy-creating-scalingpolicies-console).
   3. Under **Instance scale-in protection**, choose whether to enable instance scale-in protection. For more information, see [Use instance scale-in protection](https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-instance-protection.html).
3. (Optional) To receive notifications, for **Add notification**, configure the notification, and then choose **Next**. For more information, see [Get Amazon SNS notifications when your Auto Scaling group scales](https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-sns-notifications.html).
4. (Optional) To add tags, choose **Add tag**, provide a tag key and value for each tag, and then choose **Next**. For more information, see [Tag Auto Scaling groups and instances](https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-tagging.html).
5. On the **Review** page, choose **Create Auto Scaling group**.

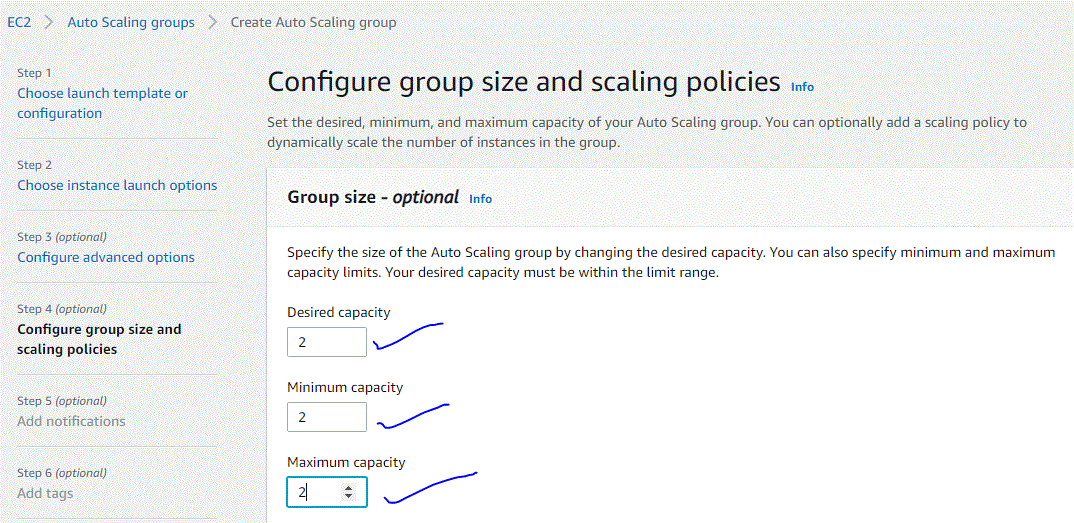










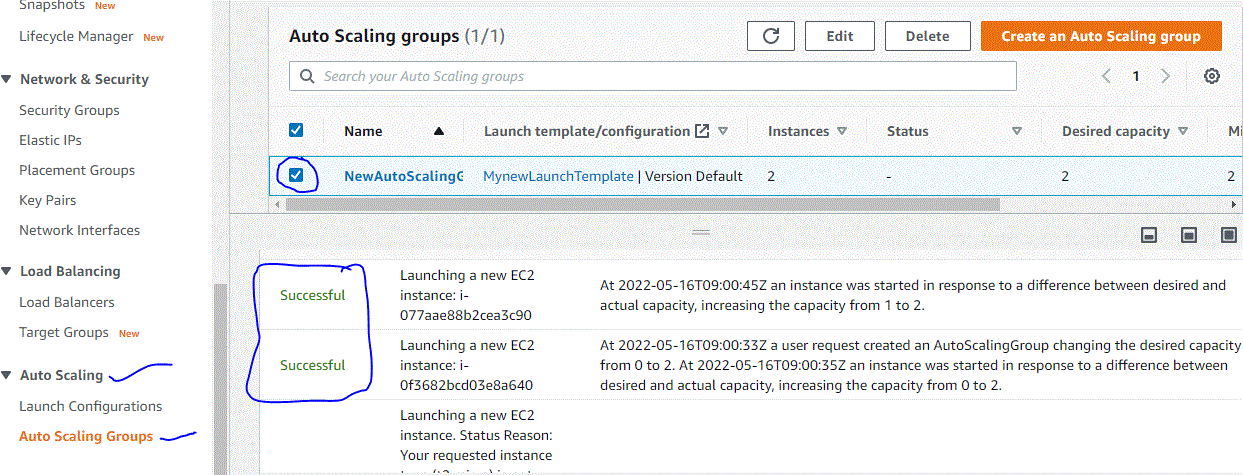












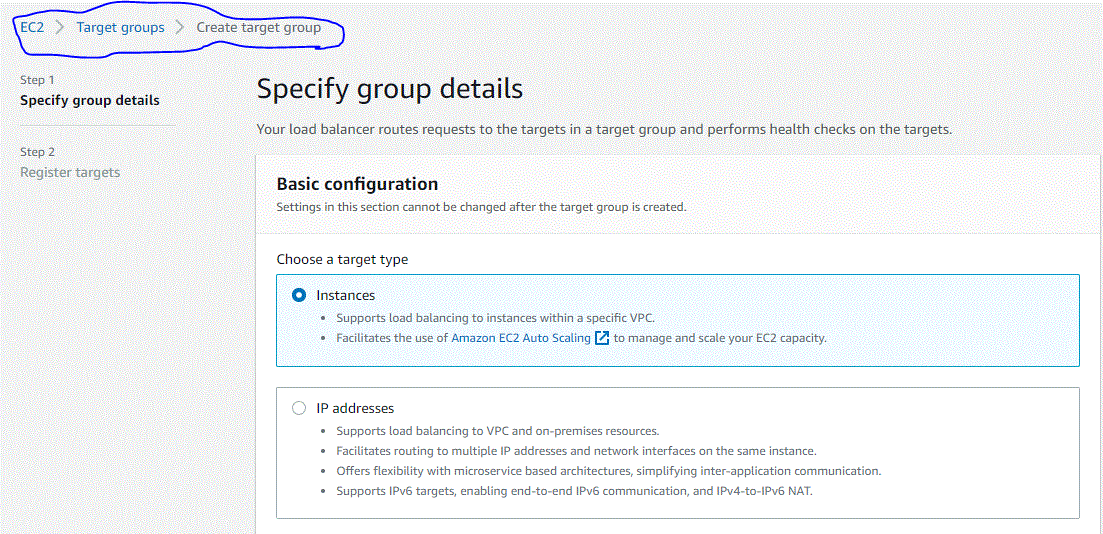
1. Hands On – Create a Target group?

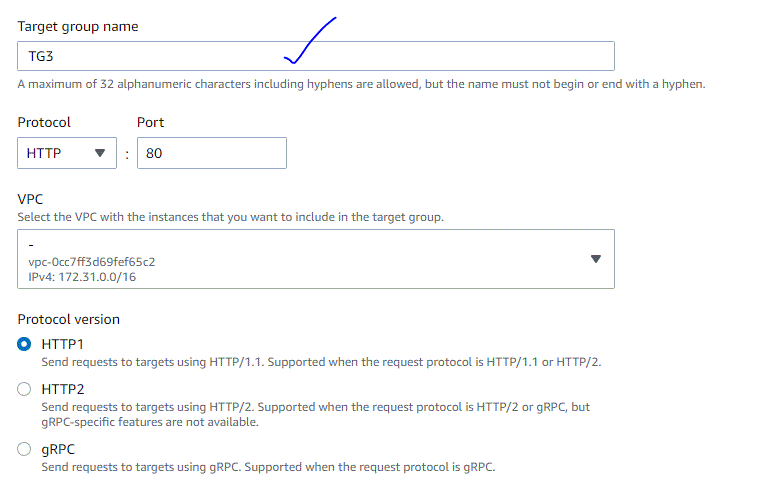
: **To create a target group using the new console**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. On the navigation pane, under **LOAD BALANCING**, choose **Target Groups**.
3. Choose **Create target group**.
4. For **Choose a target type**, select **Instances** to register targets by instance ID, **IP addresses** to register targets by IP address, or **Lambda function** to register a Lambda function as a target.
5. For **Target group name**, type a name for the target group. This name must be unique per region per account, can have a maximum of 32 characters, must contain only alphanumeric characters or hyphens, and must not begin or end with a hyphen.
6. (Optional) For **Protocol** and **Port**, modify the default values as needed.
7. If the target type is **IP addresses**, choose **IPv4** or **IPv6** as the **IP address type**, otherwise skip to the next step.

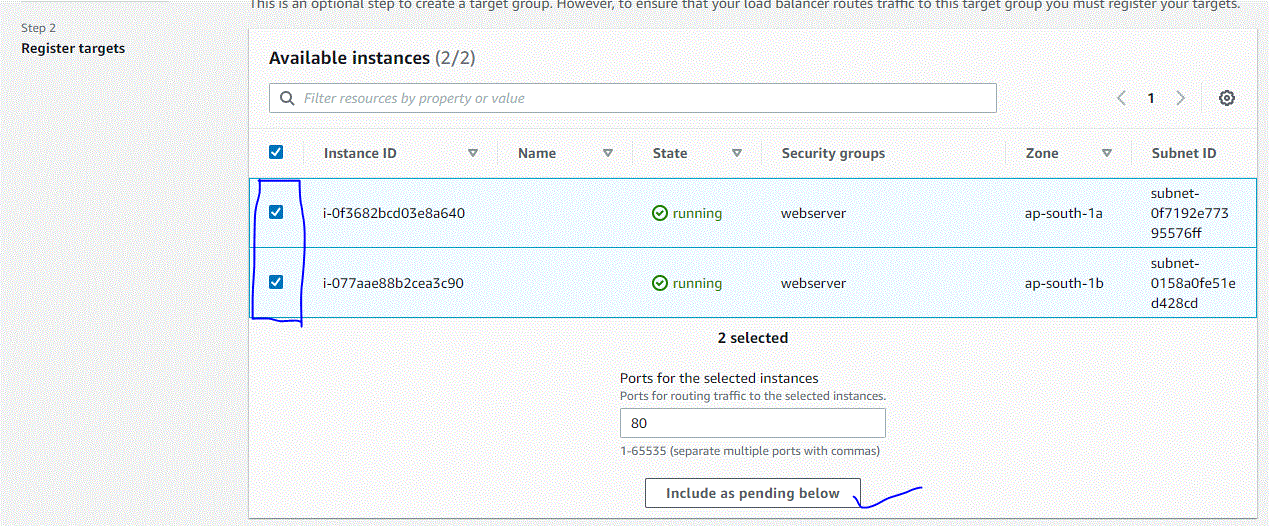
Note that only targets that have the selected IP address type can be included in this target group. The IP address type cannot be changed after the target group is created.

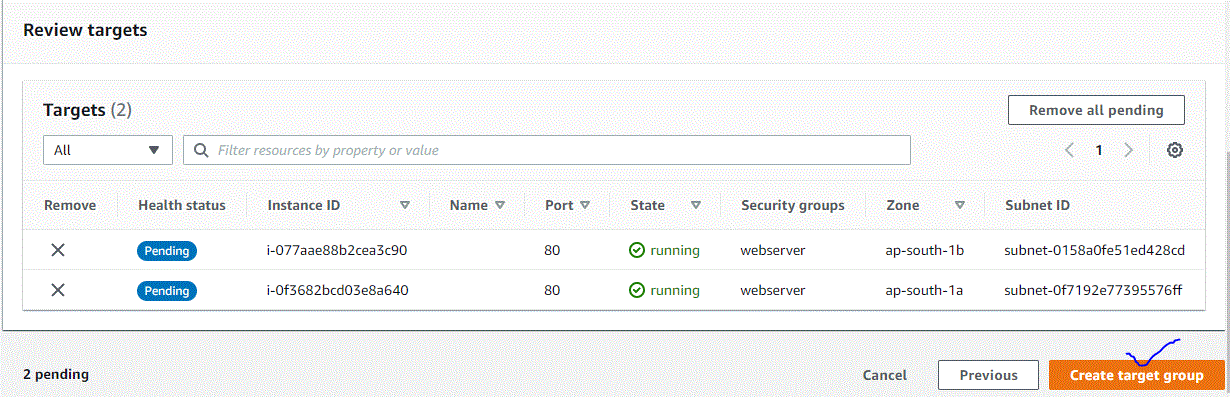
1. For **VPC**, select a virtual private cloud (VPC). Note that for **IP addresses** target types, the VPCs available for selection are those that support the **IP address type** that you chose in the previous step.
2. (Optional) For **Protocol version**, modify the default value as needed.
3. (Optional) In the **Health checks** section, modify the default settings as needed.
4. If the target type is **Lambda function**, you can enable health checks by selecting **Enable** in the **Health checks** section.
5. (Optional) Add one or more tags as follows:
   1. Expand the **Tags** section.
   2. Choose **Add tag**.
   3. Enter the tag key and the tag value.
6. Choose **Next**.
7. (Optional) Add one or more targets as follows:
   1. If the target type is **Instances**, select one or more instances, enter one or more ports, and then choose **Include as pending below**.
   2. If the target type is **IP addresses**, do the following:
      1. Select a network **VPC** from the list, or choose **Other private IP addresses**.
      2. Enter the IP address manually, or find the IP address using instance details. You can enter up to five IP addresses at a time.
      3. Enter the ports for routing traffic to the specified IP addresses.
      4. Choose **Include as pending below**.
   3. If the target type is a **Lambda function**, specify a single Lambda function or omit this step and specify a Lambda function later.
8. Choose **Create target group**.
9. (Optional) You can specify the target group in a listener rule. For more information, see [Listener Rules](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-update-rules.html).

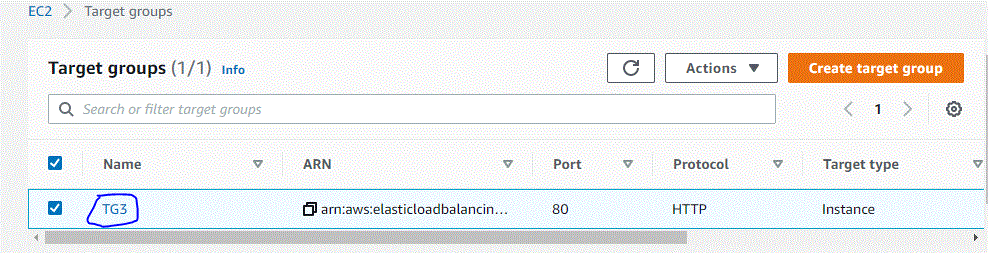


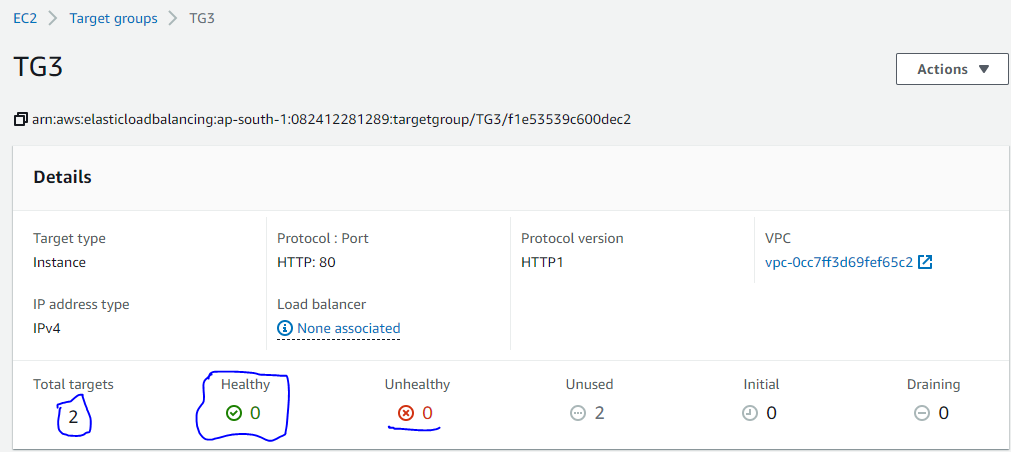












1. Hands On – Create Load Balancer?

: To create a load balancer using the AWS Management Console, complete the following tasks.

**Tasks**

* [Step 1: Configure a target group](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html#configure-target-group)
* [Step 2: Register targets](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html#select-targets)
* [Step 3: Configure a load balancer and a listener](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html#configure-load-balancer)
* [Step 4: Test the load balancer](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-application-load-balancer.html#test-load-balancer)

**Step 1: Configure a target group**

Configuring a target group allows you to register targets such as EC2 instances. The target group that you configure in this step is used as the target group in the listener rule when you configure your load balancer. For more information, see [Target groups for your Application Load Balancers](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html).

**To configure your target group**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the left navigation pane, under **Load Balancing**, choose **Target Groups**.
3. Choose **Create target group**.
4. In the **Basic configuration** section, set the following parameters:
   1. For **Choose a target type**, select **Instance** to specify targets by instance ID or **IP addresses** to specify targets by IP address. If the target type is a **Lambda function**, you can enable health checks by selecting **Enable** in the **Health checks** section.
   2. For **Target group name**, enter a name for the target group.
   3. Modify the **Port** and **Protocol** as needed.
   4. If the target type is **IP addresses**, choose **IPv4** or **IPv6** as the **IP address type**, otherwise skip to the next step.

Note that only targets that have the selected IP address type can be included in this target group. The IP address type cannot be changed after the target group is created.

* 1. For VPC, select a virtual private cloud (VPC) with the targets that you want to include in your target group.
  2. For **Protocol version**, select **HTTP1** when the request protocol is HTTP/1.1 or HTTP/2; select **HTTP2**, when the request protocol is HTTP/2 or gRPC; and select **gRPC**, when the request protocol is gRPC.

1. In the **Health checks** section, modify the default settings as needed. For **Advanced health check settings**, choose the health check port, count, timeout, interval, and specify success codes. If health checks consecutively exceed the **Unhealthy threshold** count, the load balancer takes the target out of service. If health checks consecutively exceed the **Healthy threshold** count, the load balancer puts the target back in service. For more information, see [Health checks for your target groups](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-health-checks.html).
2. (Optional) Add one or more tags as follows:
   1. Expand the **Tags** section.
   2. Choose **Add tag**.
   3. Enter the tag **Key** and tag **Value**. Allowed characters are letters, spaces, numbers (in UTF-8), and the following special characters: + - = . \_ : / @. Do not use leading or trailing spaces. Tag values are case-sensitive.
3. Choose **Next**.

**Step 2: Register targets**

You can register EC2 instances, IP addresses, or Lambda functions as targets in a target group. This is an optional step to create a load balancer. However, you must register your targets to ensure that your load balancer routes traffic to them.

1. In the **Register targets** page, add one or more targets as follows:
   * If the target type is **Instances**, select one or more instances, enter one or more ports, and then choose **Include as pending below**.
   * If the target type is **IP addresses**, do the following:
     1. Select a network **VPC** from the list, or choose **Other private IP addresses**.
     2. Enter the IP address manually, or find the IP address using instance details. You can enter up to five IP addresses at a time.
     3. Enter the ports for routing traffic to the specified IP addresses.
     4. Choose **Include as pending below**.
   * If the target type is **Lambda**, select a Lambda function, or enter a Lambda function ARN, and then choose **Include as pending below**.
2. Choose **Create target group**.

**Step 3: Configure a load balancer and a listener**

To create an Application Load Balancer, you must first provide basic configuration information for your load balancer, such as a name, scheme, and IP address type. Then, you provide information about your network, and one or more listeners. A listener is a process that checks for connection requests. It is configured with a protocol and a port for connections from clients to the load balancer. For more information about supported protocols and ports, see [Listener configuration](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#listener-configuration).

**To configure your load balancer and listener**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, under **Load Balancing**, choose **Load Balancers**.
3. Choose **Create Load Balancer**.
4. Under **Application Load Balancer**, choose **Create**.
5. **Basic configuration**
   1. For **Load balancer name**, enter a name for your load balancer. For example, **my-alb**. The name of your Application Load Balancer must be unique within your set of Application Load Balancers and Network Load Balancers for the Region. Names can have a maximum of 32 characters, and can contain only alphanumeric characters and hyphens. They can not begin or end with a hyphen, or with internal-.
   2. For **Scheme**, choose **Internet-facing** or **Internal**. An internet-facing load balancer routes requests from clients to targets over the internet. An internal load balancer routes requests to targets using private IP addresses.
   3. For **IP address type**, choose **IPv4** or **Dualstack**. Use **IPv4** if your clients use IPv4 addresses to communicate with the load balancer. Choose **Dualstack** if your clients use both IPv4 and IPv6 addresses to communicate with the load balancer.
6. **Network mapping**
   1. For **VPC**, select the VPC that you used for your EC2 instances. If you selected **Internet-facing** for **Scheme**, only VPCs with an internet gateway are available for selection.
   2. For **Mappings**, select two or more Availability Zones and corresponding subnets. Enabling multiple Availability Zones increases the fault tolerance of your applications.

For an internal load balancer, you can assign a private IP address from the IPv4 or IPv6 range of each subnet instead of letting AWS assign one for you.

Select one subnet per zone to enable. If you enabled **Dualstack** mode for the load balancer, select subnets with associated IPv6 CIDR blocks. You can specify one of the following:

* + - Subnets from two or more Availability Zones
    - Subnets from one or more Local Zones
    - One Outpost subnet

1. For **Security groups**, select an existing security group, or create a new one.

The security group for your load balancer must allow it to communicate with registered targets on both the listener port and the health check port. The console can create a security group for your load balancer on your behalf with rules that allow this communication. You can also create a security group and select it instead. For more information, see [Recommended rules](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-update-security-groups.html#security-group-recommended-rules).

(Optional) To create a new security group for your load balancer, choose **Create a new security group**.

1. For **Listeners and routing**, the default listener accepts HTTP traffic on port 80. You can keep the default protocol and port, or choose different ones. For **Default action**, choose the target group that you created. You can optionally choose **Add listener** to add another listener (for example, an HTTPS listener).

If you create an HTTPS listener, configure the required **Secure listener settings**. Otherwise, go to the next step.

When you use HTTPS for your load balancer listener, you must deploy an SSL certificate on your load balancer. The load balancer uses this certificate to terminate the connection and decrypt requests from clients before sending them to the targets. For more information, see [SSL certificates](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html#https-listener-certificates). Additionally, specify the security policy that the load balancer uses to negotiate SSL connections with the clients. For more information, see [Security policies](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html#describe-ssl-policies).

For **Default SSL certificate**, do one of the following:

* 1. If you created or imported a certificate using AWS Certificate Manager, select **From ACM**, and then select the certificate.
  2. If you uploaded a certificate using IAM, select **From IAM**, and then select the certificate.
  3. If you want to import a certificate to ACM or IAM , enter a certificate name. Then, paste the PEM-encoded private key and body.

1. (Optional) You can use **Add-on services**, such as the **AWS Global Accelerator** to create an accelerator and associate the load balancer with the accelerator. The accelerator name can have up to 64 characters. Allowed characters are a-z, A-Z, 0-9, . and - (hyphen). Once the accelerator is created, you can use the **AWS Global Accelerator** console to manage it.
2. **Tag and create**
   1. (Optional) Add a tag to categorize your load balancer. Tag keys must be unique for each load balancer. Allowed characters are letters, spaces, numbers (in UTF-8), and the following special characters: + - = . \_ : / @. Do not use leading or trailing spaces. Tag values are case-sensitive.
   2. Review your configuration, and choose **Create load balancer**. A few default attributes are applied to your load balancer during creation. You can view and edit them after creating the load balancer. For more information, see [Load balancer attributes](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/application-load-balancers.html#load-balancer-attributes).

**Step 4: Test the load balancer**

After creating your load balancer, you can verify that your EC2 instances pass the initial health check. You can then check that the load balancer is sending traffic to your EC2 instance. To delete the load balancer, see [Delete an Application Load Balancer](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-delete.html).

**To test the load balancer**

1. After the load balancer is created, choose **Close**.
2. In the navigation pane, under **Load Balancing**, choose **Target Groups**.
3. Select the newly created target group.
4. Choose **Targets** and verify that your instances are ready. If the status of an instance is initial, it's typically because the instance is still in the process of being registered. This status can also indicate that the instance has not passed the minimum number of health checks to be considered healthy. After the status of at least one instance is healthy, you can test your load balancer. For more information, see [Target health status](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-health-checks.html#target-health-states).
5. In the navigation pane, under **Load Balancing**, choose **Load Balancers**.
6. Select the newly created load balancer.
7. Choose **Description** and copy the DNS name of the load balancer (for example, my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com). Paste the DNS name into the address field of an internet-connected web browser. If everything is working, the browser displays the default page of your server.

