

## AWS SES Configuration

In this tutorial we will configure the components required by Amazon SES (Simple Email Service) to allow us to send outbound emails from an EC2 instance.

### Prerequisites

- an AWS Free Tier account
- AWS Ubuntu 20 EC2 instance
- AWS RHEL 8 EC2 instance
- an email address
- internet access

If you do not have an AWS account, you can access my **AWS Create Free Tier Account** tutorial [here](#).

If you do not have an AWS Ubuntu 20 EC2 instance, my tutorial **Create AWS Ubuntu 20 EC2 Instance** is [here](#). If you do not have an AWS RHEL 8 EC2 instance, my tutorial **Create AWS RHEL 8 EC2 Instance** is [here](#).

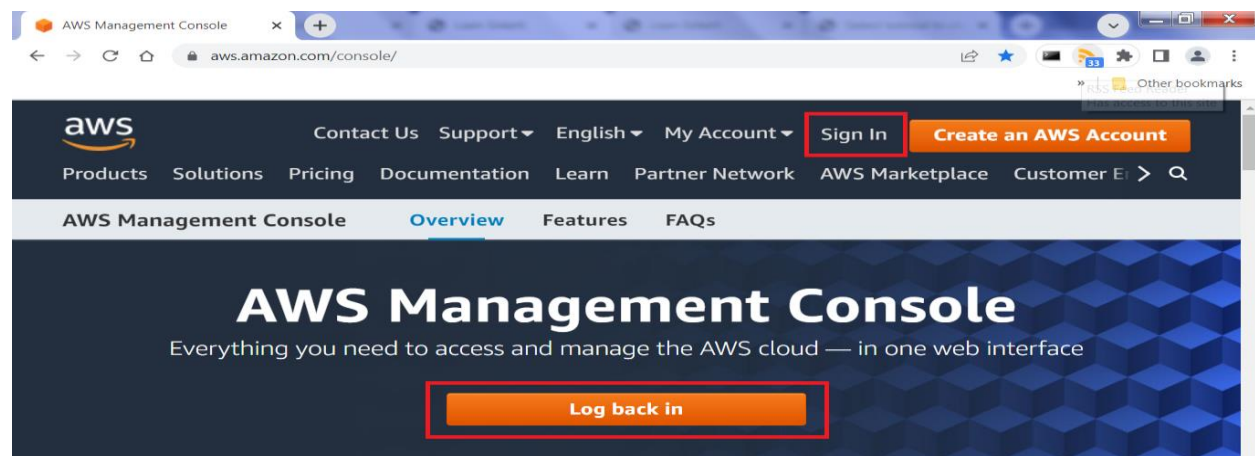
After completing this tutorial, you will be ready for my Postfix tutorials where I demonstrate the installation, and configuration, of Postfix as an outbound send-only email server, on an Ubuntu 20 EC2 & RHEL 8 EC2. Postfix will allow you to fully utilize Amazon SES.

The **AWS Ubuntu 20 EC2 Postfix Install** tutorial is accessible [here](#), while the **AWS RHEL 8 EC2 Postfix Install** tutorial is accessible [here](#).

Steps to complete tutorial:

- [Gather EC2 Instance Information](#)
- [Change EC2 Instance Security Group](#)
- [Add Rule to Security Group](#)
- [Create Verified Identity](#)
- [Create SMTP Credentials](#)
- [Create VPC Endpoint](#)
- [Simple Email Service Test](#)

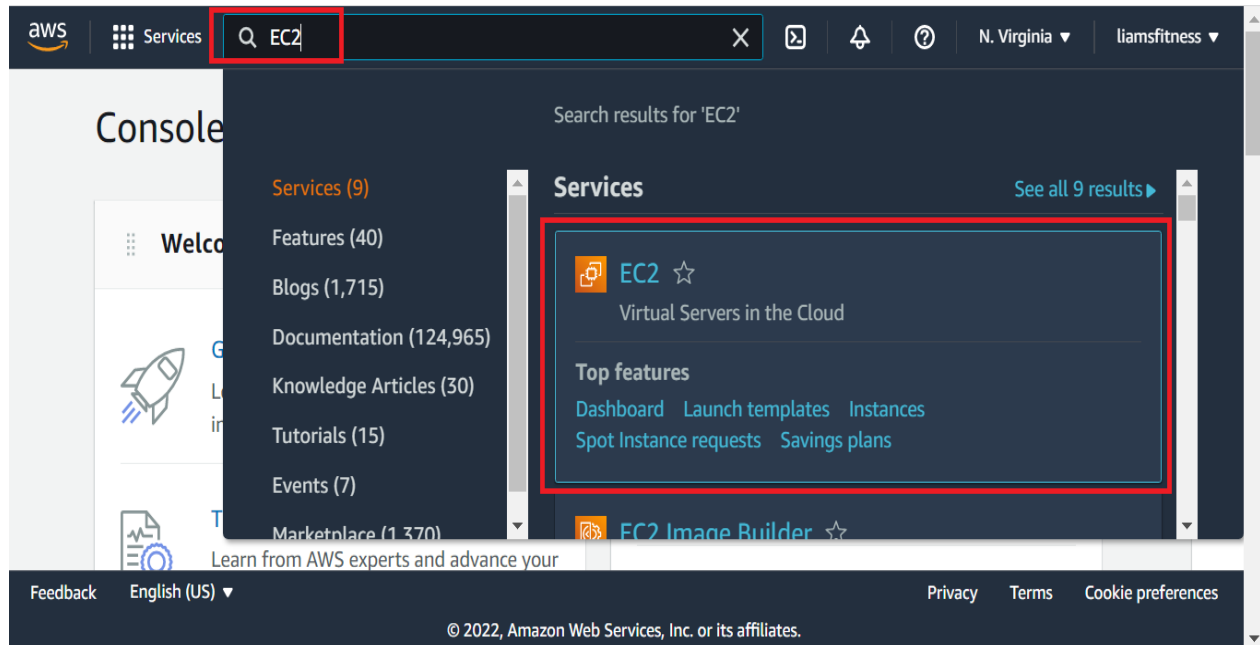
To begin, go to the following website, <https://aws.amazon.com/console/> and log in to the console.



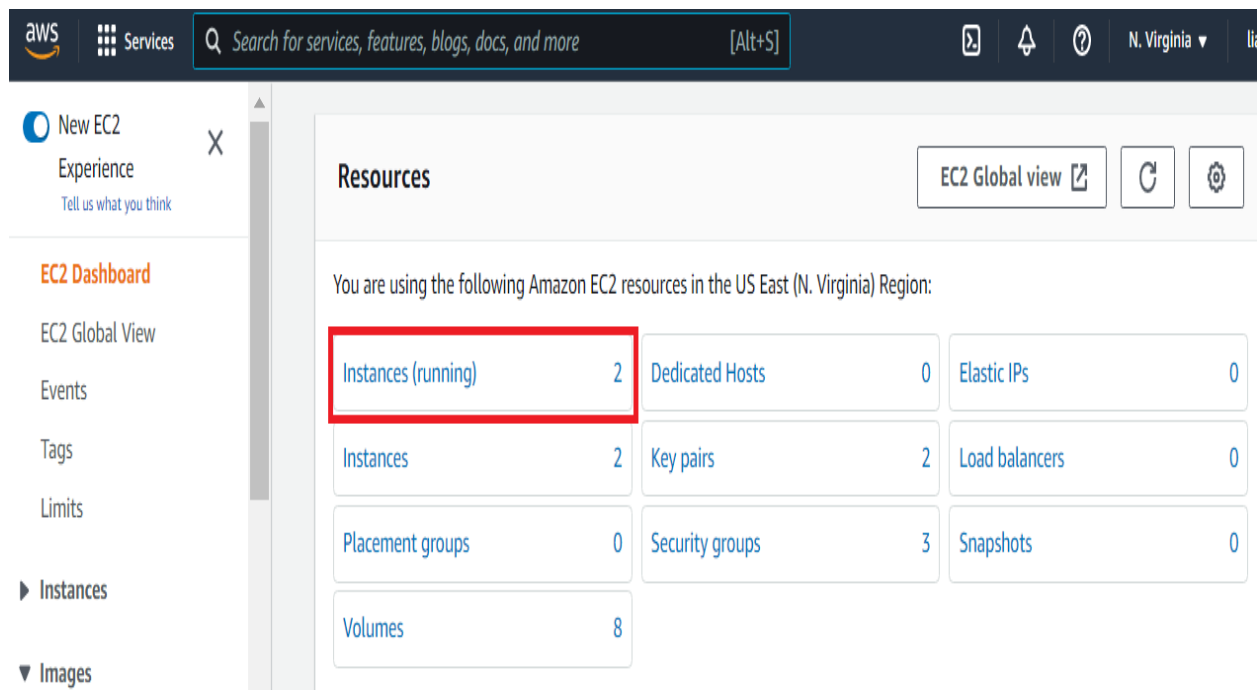
Before we configure the Amazon Simple Email Service, I will first gather the necessary information from both my EC2 instances: **security group, subnet & availability zone**. All of these values will be used during the VPC Endpoint creation, while the subnet will also be used when adding a new inbound rule to the security group.

## Gather EC2 Instance Information

Once logged in, enter **EC2** in the search bar and select **EC2 Virtual Servers in the Cloud**.



On the EC2 Dashboard, select **Instances (running)**



On the Instances screen, ensure an EC2 instance is selected and that the **Security** tab is selected. I will start with my Ubuntu 20 EC2 instance (**u20\_vm**).

The screenshot shows the AWS Management Console interface. On the left sidebar, the 'Instances' link is selected. The main panel displays a list of instances under the heading 'Instances (1/2) Info'. A filter 'Instance state = running' is applied. Two instances are listed: 'rh8\_vm' and 'u20\_vm'. The 'u20\_vm' instance is selected, highlighted with a red box. Below the list, the details for 'Instance: i-0119d3a3b1beafcfc (u20\_vm)' are shown. The 'Security' tab is selected and highlighted with a red box. Under 'Security details', the 'IAM Role' is '-', 'Owner ID' is '572092638768', and 'Launch time' is 'Sun Jul 17 2022 11:41:29 GMT-0400 (Eastern Daylight Time)'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-0119d3a3b1beafcfc (u20\_vm)

Security details

IAM Role	Owner ID	Launch time
-	572092638768	Sun Jul 17 2022 11:41:29 GMT-0400 (Eastern Daylight Time)

In the bottom section of the screen, scroll down until **Security groups** is visible and note the value. In my case the value is **security-group1**.

The screenshot shows the AWS Management Console interface, similar to the previous one. The 'u20\_vm' instance is still selected. In the details panel for 'Instance: i-0119d3a3b1beafcfc (u20\_vm)', the 'Security groups' section is visible and highlighted with a red box. It shows 'sg-02520767438262038 (security-group1)'. Below this, the 'Inbound rules' section is partially visible.

Instance: i-0119d3a3b1beafcfc (u20\_vm)

Security groups

sg-02520767438262038 (security-group1)

Inbound rules

Next, in the bottom of the screen, scroll back up until the tabbed menu is visible and select the **Networking** tab.

The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with options like 'New EC2 Experience', 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances', 'Images', 'AMI Catalog', and 'Elastic Block Store'. The main content area is titled 'Instances (1/2)' and shows a table of running instances. The instance 'u20\_vm' with ID 'i-0119d3a3b1beafcfc' is selected and highlighted with a red box. Below the table, the 'Networking' tab is selected and highlighted with a red box. A message states: 'You can now check network connectivity with Reachability Analyzer.' with a 'Run Reachability Analyzer' button. Below this, the 'Networking details' section is partially visible.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-0119d3a3b1beafcfc (u20\_vm)

Details | Security | **Networking** | Storage | Status checks | Monitoring | Tags

You can now check network connectivity with Reachability Analyzer. [Run Reachability Analyzer](#)

Networking details Info

In the bottom section of the screen, under the **Networking** tab, scroll down until **Subnet ID** and **Availability zone** are visible and note the values. In my case the values are **subnet\_default** & **us-east-1b**

This screenshot shows the 'Networking details' section for the selected instance 'u20\_vm'. The 'Subnet ID' is 'subnet-0096efb1b7740b3da (subnet\_default)' and the 'Availability zone' is 'us-east-1b', both highlighted with red boxes. Other details like 'IPv6 addresses', 'Secondary private IPv4 addresses', 'Carrier IP addresses (ephemeral)', and 'Outpost ID' are also visible.

Instance: i-0119d3a3b1beafcfc (u20\_vm)

Subnet ID subnet-0096efb1b7740b3da (subnet_default)	IPv6 addresses -	Secondary private IPv4 addresses -
Availability zone us-east-1b	Carrier IP addresses (ephemeral) -	Outpost ID -

Now I will perform the same steps to gather information on my RHEL 8 EC2 instance (**rh8\_vm**).

On the Instances screen, I will select **rh8\_vm** and ensure that the **Security** tab is selected.

The screenshot shows the AWS Management Console interface. On the left sidebar, the 'Instances' section is expanded. The main content area displays a list of instances. The instance 'rh8\_vm' with ID 'i-052cd6fd1db5e4114' is selected and highlighted with a red box. Below the list, the details for this instance are shown, with the 'Security' tab selected and highlighted with a red box. The 'Security details' section shows the IAM Role as '-', the Owner ID as '572092638768', and the Launch time as 'Sun Jul 17 2022 11:41:45 GMT-0400 (Eastern Daylight Time)'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-052cd6fd1db5e4114 (rh8\_vm)

Details | **Security** | Networking | Storage | Status checks | Monitoring | Tags

▼ Security details

IAM Role	Owner ID	Launch time
-	572092638768	Sun Jul 17 2022 11:41:45 GMT-0400 (Eastern Daylight Time)

In the bottom section of the screen, scroll down until **Security groups** is visible and note the value. In my case the value is **security-group2**.

The screenshot shows the AWS Management Console interface. On the left sidebar, the 'Instances' section is expanded. The main content area displays a list of instances. The instance 'rh8\_vm' with ID 'i-052cd6fd1db5e4114' is selected and highlighted with a red box. Below the list, the details for this instance are shown, with the 'Security' tab selected and highlighted with a red box. The 'Security groups' section is highlighted with a red box, showing the value 'sg-0a1d0061cebed314b (security-group2)'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-052cd6fd1db5e4114 (rh8\_vm)

Details | **Security** | Networking | Storage | Status checks | Monitoring | Tags

▼ Security groups

sg-0a1d0061cebed314b (security-group2)

▼ Inbound rules

Next, in the bottom of the screen, scroll back up until the tabbed menu is visible and select the **Networking** tab.

The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with options like 'New EC2 Experience', 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances', 'Images', 'AMI Catalog', and 'Elastic Block Store'. The main content area is titled 'Instances (1/2) Info'. It features a search bar, a filter 'Instance state = running', and a table of instances. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, and Alarm status. Two instances are listed: 'rh8\_vm' (ID: i-052cd6fd1db5e4114) and 'u20\_vm' (ID: i-0119d3a3b1beafcfc), both in a 'Running' state. The 'rh8\_vm' row is selected. Below the table, the details for 'Instance: i-052cd6fd1db5e4114 (rh8\_vm)' are shown. A tabbed menu at the top of the details section includes 'Details', 'Security', 'Networking' (which is selected and highlighted with a red box), 'Storage', 'Status checks', 'Monitoring', and 'Tags'. A message states 'You can now check network connectivity with Reachability Analyzer.' with a 'Run Reachability Analyzer' button. Below this, the 'Networking details' section is partially visible.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

In the bottom section of the screen, under the **Networking** tab, scroll down until **Subnet ID** and **Availability zone** are visible and note the values. In my case the values are **subnet\_default** & **us-east-1b**.

This screenshot shows the 'Networking' tab for the same EC2 instance 'rh8\_vm'. The 'Subnet ID' is 'subnet-0096efb1b7740b3da' (labeled as 'subnet\_default') and the 'Availability zone' is 'us-east-1b'. Both fields are highlighted with red boxes. Other networking details like 'IPv6 addresses', 'Secondary private IPv4 addresses', 'Carrier IP addresses (ephemeral)', and 'Outpost ID' are also visible but empty.

Subnet ID	IPv6 addresses	Secondary private IPv4 addresses
subnet-0096efb1b7740b3da (subnet_default)	-	-

Availability zone	Carrier IP addresses (ephemeral)	Outpost ID
us-east-1b	-	-

After gathering the necessary EC2 instance information, we need to open a port (587) through the firewall by adding an inbound rule to the security group (**security-group1**). One of the required rule parameters is the **Source** field (*from where these requests will be coming from*). The value I will be using is the CIDR IPv4 subnet of both my EC2 instances. To access this value, click the link under the **Subnet ID**

The screenshot shows the AWS Management Console interface. On the left, there's a navigation menu with options like 'New EC2 Experience', 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances', 'Images', 'AMIs', 'AMI Catalog', 'Elastic Block Store', and 'Volumes'. The main content area displays 'Instances (1/2) Info'. A table lists two instances: 'rh8\_vm' (ID: i-052cd6fd1db5e4114) and 'u20\_vm' (ID: i-0119d3a3b1beafcfc). Both are in a 'Running' state. Below the table, the details for instance 'rh8\_vm' are shown. A red box highlights the 'Subnet ID' field, which contains the value 'subnet-0096efb1b7740b3da (subnet\_default)' with a link icon.

The **Subnets** screen will open in a new tab. On the **Subnets** screen, scroll to the right until the **IPv4 CIDR** heading is visible and note the value.

The screenshot shows the AWS Management Console interface for the 'Subnets' section. The top navigation bar is the same as the previous screenshot. The main content area displays 'Subnets (1/1) Info'. A table lists one subnet: 'subnet\_default' (ID: subnet-0096efb1b7740b3da) in an 'Available' state, associated with VPC 'vpc-01ac0d160f388c36e'. Below the table, the details for the subnet are shown. A red box highlights the 'IPv4 CIDR' field, which contains the value '172.31.0.0/20'.

In my case, the **IPv4 CIDR** value is **172.31.0.0/20**.

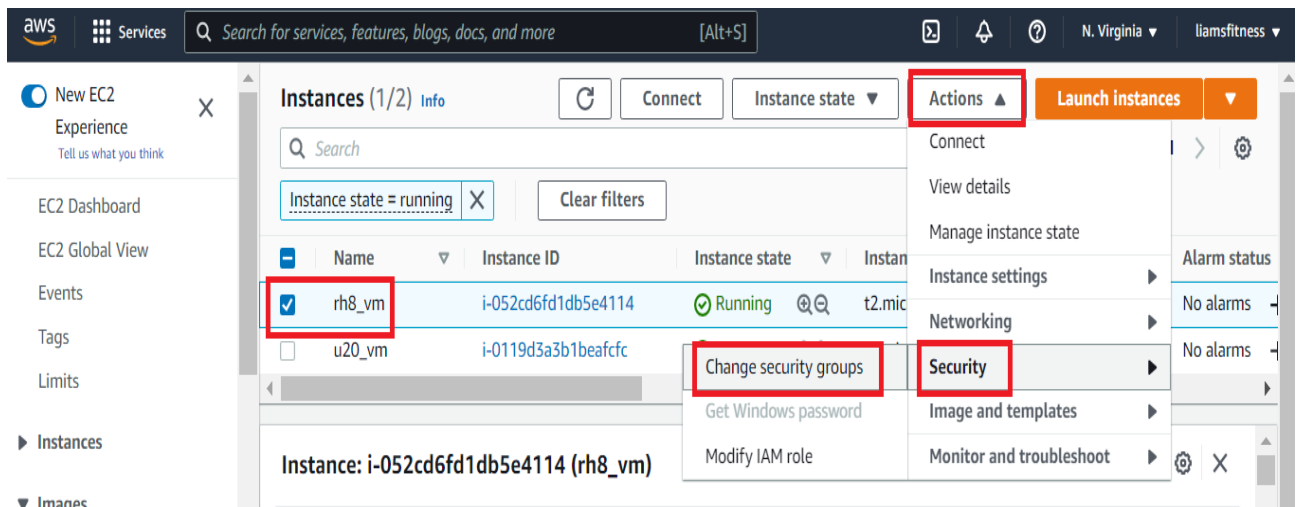


At the end of this tutorial, I want both of my EC2 instances to be able to send outbound emails. Normally, port 25 is used to send email. Unfortunately, Amazon prevents the use of port 25. Instead, we will use port 587. Therefore, we will need to add an inbound rule for port 587 to the security group (**security-group1**). Since my RHEL 8 EC2 instance is using **security-group2**, I will first change its security group to **security-group1**. This will prevent me from having to add separate rules to different security groups.

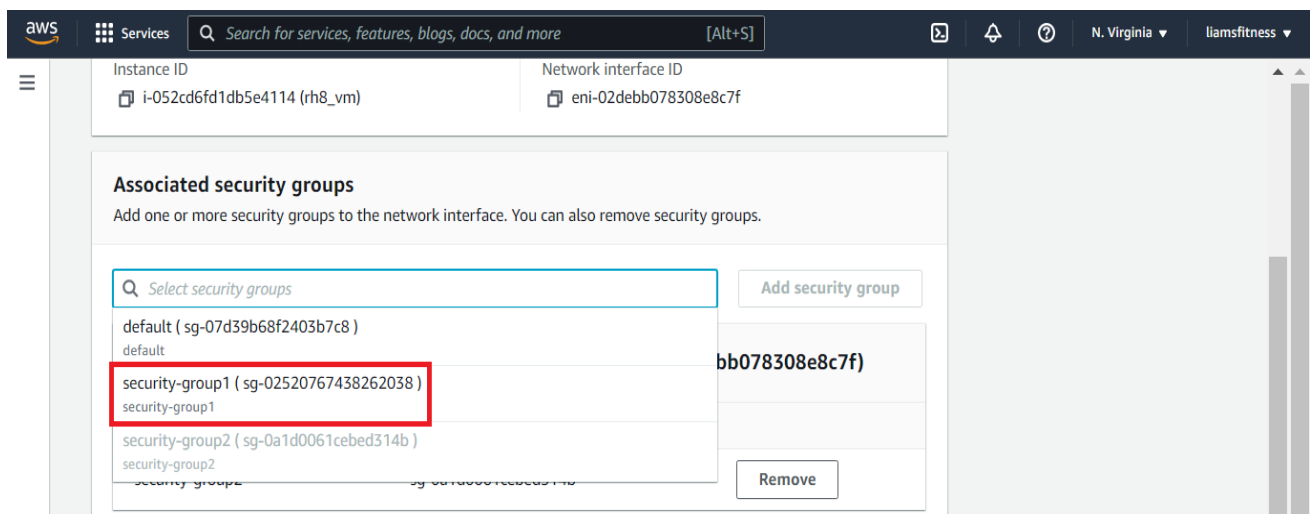
After making that change and adding a new inbound rule to **security-group1**, both EC2 instances will be capable of sending outbound emails.

## Change EC2 Instance Security Group

Back on the **Instances** screen, to change my RHEL 8 EC2 instance's security group, I will first ensure it is selected. Then, I will click the **Actions** menu, scroll down and click **Security** followed by **change security groups**.



On the **Change security groups** screen, scroll down to the Associated security groups section and place your cursor in the greyed out **Select security groups** text box. A listing of available security groups will appear. I have selected **security-group1**





Next, click **Add security group**

**Associated security groups**  
Add one or more security groups to the network interface. You can also remove security groups.

Q

sg-02520767438262038

X

Add security group

Then, next to the original security group (**security-group2**) click **Remove**

**Associated security groups**  
Add one or more security groups to the network interface. You can also remove security groups.

Q

sg-02520767438262038

X

Add security group

**Security groups associated with the network interface (eni-02debb078308e8c7f)**

Security group name	Security group ID	
security-group2	sg-0a1d0061cebed314b	Remove
security-group1	sg-02520767438262038	Remove

Finally, to save the changes, click **Save**

**Associated security groups**  
Add one or more security groups to the network interface. You can also remove security groups.

Q

sg-02520767438262038

X

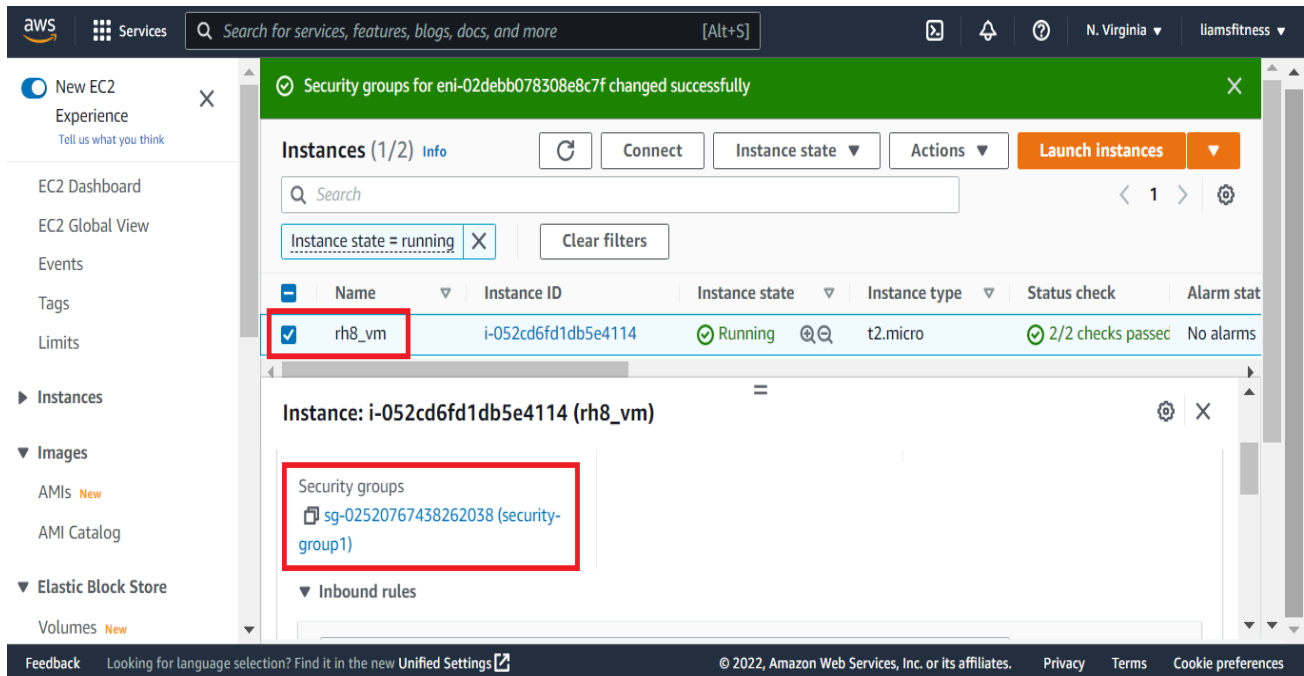
Add security group

**Security groups associated with the network interface (eni-02debb078308e8c7f)**

Security group name	Security group ID	
security-group1	sg-02520767438262038	Remove

Cancel

Save

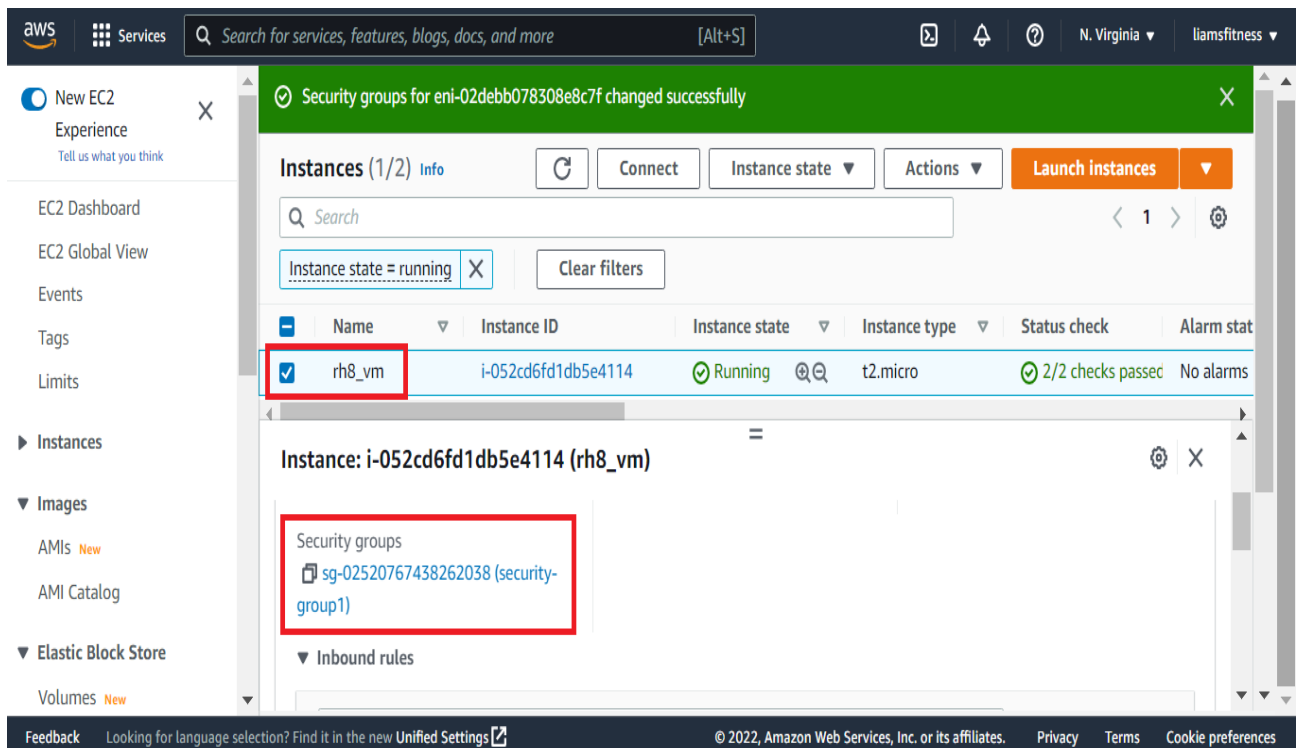


The security group is now the same for both of my EC2 instances: **security-group1**

The next step is to add an inbound rule for port 587 to **security-group1**.

### Add Rule to Security Group

To access the **Security Groups** screen, at the bottom of the **Instances** screen, under the **Security** tab, locate **Security groups** and click the security group link (in my case, **security-group1**).



On the **security-group1** screen, scroll down until the **Inbound rules** section is completely visible.

The screenshot shows the AWS Management Console interface for a security group. The breadcrumb navigation indicates the path: EC2 > Security Groups > sg-02520767438262038 - security-group1. The main heading is 'sg-02520767438262038 - security-group1'. Below this is a 'Details' section with a table of properties:

Security group name	Security group ID	Description	VPC ID
security-group1	sg-02520767438262038	Limit access to instance	vpc-01ac0d160f388c36e
Owner	Inbound rules count	Outbound rules count	
572092638768	5 Permission entries	1 Permission entry	

Below the details section are three tabs: 'Inbound rules' (highlighted with a red box), 'Outbound rules', and 'Tags'. The left sidebar contains navigation options like 'New EC2 Experience', 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances', 'Images', 'AMI Catalog', 'Elastic Block Store', and 'Volumes'.

Next, click **Edit Inbound Rules**

This screenshot shows the 'Inbound rules' section of the security group. At the top, there are three tabs: 'Inbound rules' (active), 'Outbound rules', and 'Tags'. A notification banner states: 'You can now check network connectivity with Reachability Analyzer' with a 'Run Reachability Analyzer' button. Below the notification, the section is titled 'Inbound rules (3)'. There are three buttons: a refresh icon, 'Manage tags', and 'Edit inbound rules' (highlighted with a red box). A search bar labeled 'Filter security group rules' is present. Below is a table of inbound rules:

<input type="checkbox"/>	Name	Security group rule...	IP version	Type
<input type="checkbox"/>	-	sgr-0be85105ca435d1...	IPv4	HTTP
<input type="checkbox"/>	-	sgr-0ee1cf6505bb75643	IPv4	HTTPS
<input type="checkbox"/>	-	sgr-05aa0248d0edfc4eb	IPv4	SSH

On the **Edit Inbound Rules** screen, click **Add rule**

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>		
sgr-0be85105ca435d1e8	HTTP ▼	TCP	80	Custom ▼	<input type="text" value="Q"/>	<input type="text"/>	Del ete
					0.0.0.0/0 ✕		
sgr-0ee1cf6505bb75643	HTTPS ▼	TCP	443	Custom ▼	<input type="text" value="Q"/>	<input type="text"/>	Del ete
					0.0.0.0/0 ✕		
sgr-05aa0248d0edfc4eb	SSH ▼	TCP	22	Custom ▼	<input type="text" value="Q"/>	<input type="text"/>	Del ete
					0.0.0.0/0 ✕		

**Add rule**

Ensure the **Port range** is set to **587** and **Source** is set to **172.31.0.0/20** and click **Save rules**.

Custom TCP ▼

TCP

587

Custom ▼

Del ete

172.31.0.0/20 ✕

**Add rule**

CancelPreview changes**Save rules**

Inbound rules (4)

Manage tagsEdit inbound rules

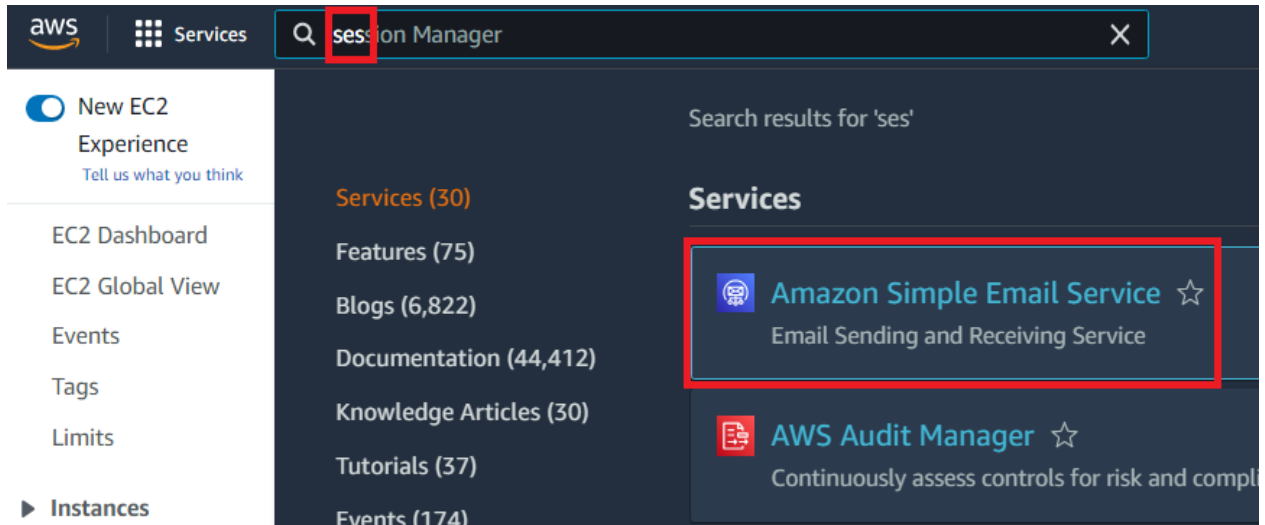
< 1 > ⚙

Security group rule ID	IP version	Type	Protocol	Port range	Source
sgr-0be85105ca435d1e8	IPv4	HTTP	TCP	80	0.0.0.0/0
sgr-03e80f770360d9f6f	IPv4	Custom TCP	TCP	587	172.31.0.0/20
sgr-0ee1cf6505bb75643	IPv4	HTTPS	TCP	443	0.0.0.0/0
sgr-05aa0248d0edfc4eb	IPv4	SSH	TCP	22	0.0.0.0/0

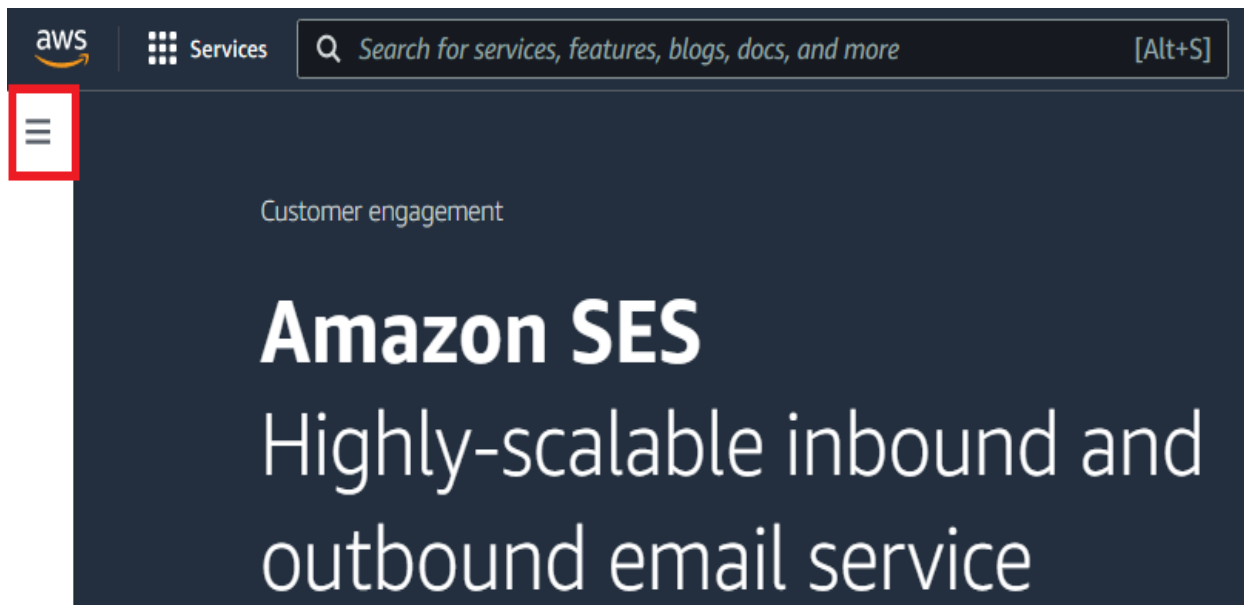
## Create Verified Identity

In order to use the Amazon's SES (Simple Email Service), the first step is to create a verified identity which can be either a domain or an email address. I will be creating a verified identity using an email address.

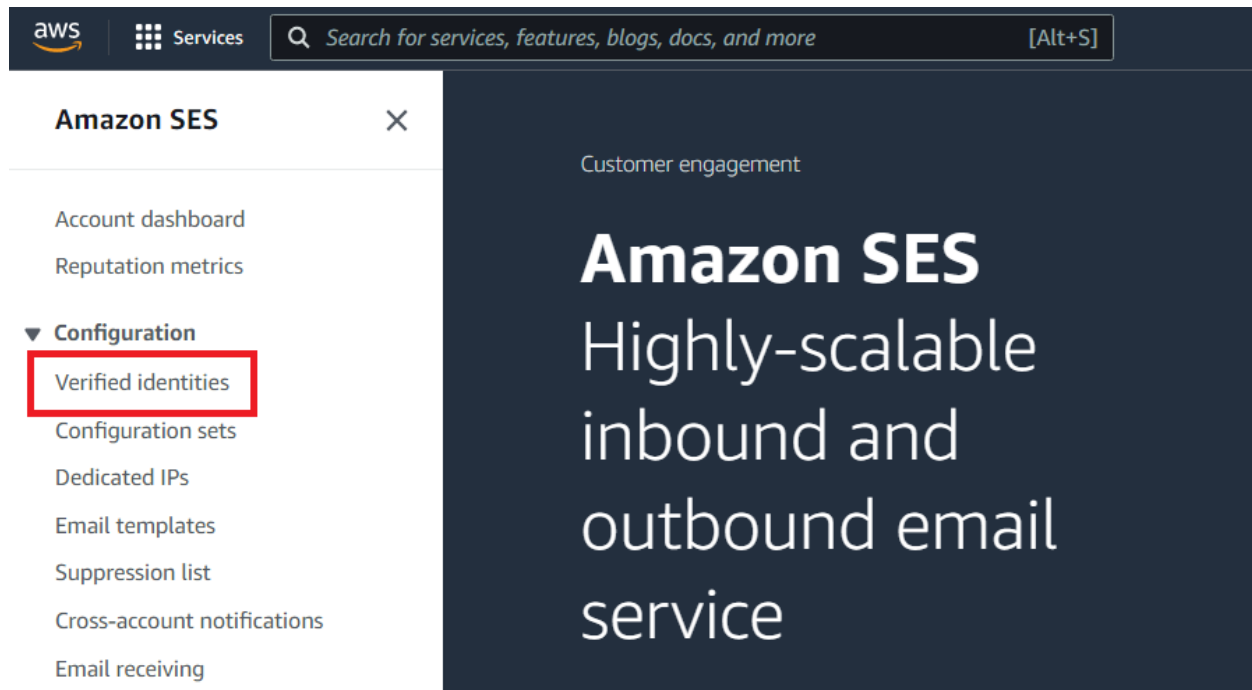
To access the SES service, at the top of the screen, type **ses** in the search bar and select **Amazon Simple Email Service**.



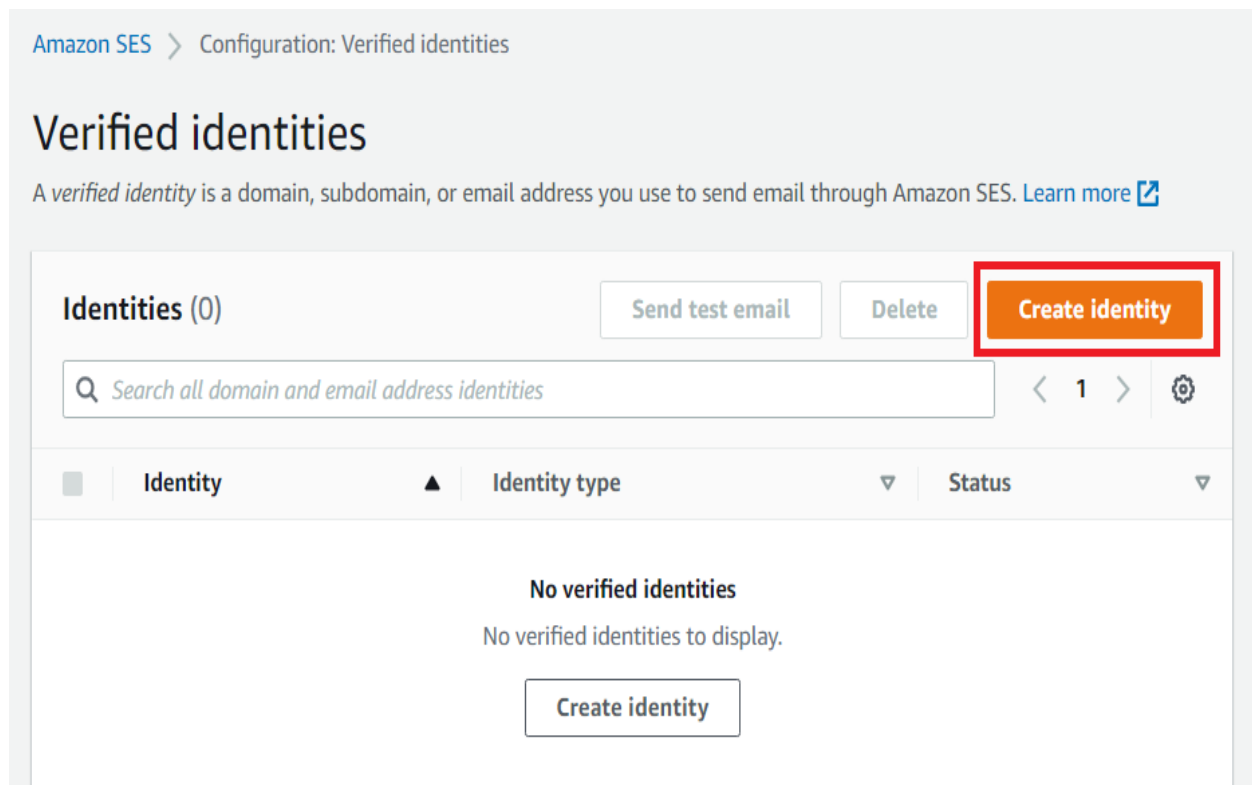
On the SES screen, click the accordion menu in the top left of the screen to access the available options.



Under **Configuration**, click **Verified Identities**



On the **Verified identities** screen, click **Create identity**



On the **Create Identity** screen, select **Email address**, then enter your email address and leave **Assign a default configuration set** unchecked.

## Create identity

A *verified identity* is a domain, subdomain, or email address you use to send email through Amazon SES. Identity verification at the domain level extends to all email addresses under one verified domain identity.

### Identity details [Info](#)

#### Identity type

☐

Domain

To verify ownership of a domain, you must have access to its DNS settings to add the necessary records.

☒

Email address

To verify ownership of an email address, you must have access to its inbox to open the verification email.

#### Email address

liams.fitness@gmail.com

Email address can contain up to 320 characters, including plus signs (+), equals signs (=) and underscores (\_).

☐

Assign a default configuration set

Enabling this option ensures that the assigned configuration set is applied to messages sent from this identity by default whenever a configuration set isn't specified at the time of sending.

You can add a Tag if you wish, I have not. Finally, click **Create identity**

### Tags - optional [Info](#)

You can add one or more tags to help manage and organize your resources, including identities.

No tags associated with the resource.

Add new tag


You can add 50 more tags.

Cancel

Create identity



A verification email will be sent from **Amazon Web Services** which must be confirmed in order for the email identity to be verified.

 **Action required**


To verify ownership of this identity, check your inbox for a verification request email and click the link provided.

Resend

Amazon SES > Configuration: Verified identities > liams.fitness@gmail.com



liams.fitness@gmail.com

DeleteSend test email

 **Legacy TXT records**

Domain verification in Amazon SES is now based on *DomainKeys Identified Mail (DKIM)*, an email authentication standard that receiving mail servers use to validate an email's authenticity. Configuring DKIM in your domain's DNS settings confirms to SES that you're the identity owner, eliminating the need for TXT records. Domain identities that were verified using TXT records do not need to be reverified; however, we still recommend enabling DKIM signatures to enhance the deliverability of your mail with DKIM-compliant email providers. To access your legacy TXT records, download Legacy TXT record set as .csv [📄](#).

Summary for liams.fitness@gmail.com

Identity status	Amazon Resource Name (ARN)	AWS Region
 Unverified	 arn:aws:ses:us-east-1:572092638768:identity/liams.fitness@gmail.com	US East (N. Virginia)

Open your email client and click the link provided to verify your email identity.

From Amazon Web Services <no-reply-aws@amazon.com> ☆

ReplyForwardArchiveJunkDeleteMore

Subject Amazon Web Services – Email Address Verification Request in region US East (N. Virginia) 10:07 a.m.

To Me <liams.fitness@gmail.com> ☆

Dear Amazon Web Services Customer,

We have received a request to authorize this email address for use with Amazon SES and Amazon Pinpoint in region US East (N. Virginia). If you requested this verification, please go to the following URL to confirm that you are authorized to use this email address:

[https://email-verification.us-east-1.amazonaws.com/?Context=572092638768&X-Amz-Date=20220718T140702Z&Identity.IdentityName=liams.fitness%40gmail.com&X-Amz-Algorithm=AWS4-HMAC-SHA256&Identity.IdentityType=EmailAddress&X-Amz-SignedHeaders=host&X-Amz-Credential=AKIAVM67ZIEFRDECB3HF%2F20220718%2Fus-east-1%2Fses%2Faws4\\_request&Operation=ConfirmVerification&Namespace=Bacon&X-Amz-Signature=7ad415433d04e4bfafd2ccb0606483515dcd3321f1ef09f2c6fda42e924e1d4d](https://email-verification.us-east-1.amazonaws.com/?Context=572092638768&X-Amz-Date=20220718T140702Z&Identity.IdentityName=liams.fitness%40gmail.com&X-Amz-Algorithm=AWS4-HMAC-SHA256&Identity.IdentityType=EmailAddress&X-Amz-SignedHeaders=host&X-Amz-Credential=AKIAVM67ZIEFRDECB3HF%2F20220718%2Fus-east-1%2Fses%2Faws4_request&Operation=ConfirmVerification&Namespace=Bacon&X-Amz-Signature=7ad415433d04e4bfafd2ccb0606483515dcd3321f1ef09f2c6fda42e924e1d4d)

Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification request.

If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phishing attempt, but either a misunderstanding of how to use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully communicated the procedure first. If you are still concerned, please forward this notification to [aws-email-domain-verification@amazon.com](mailto:aws-email-domain-verification@amazon.com) and let us know in the forward that you did not request the verification.

To learn more about sending email from Amazon Web Services, please refer to the Amazon SES Developer Guide at <http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html> and Amazon Pinpoint Developer Guide at <http://docs.aws.amazon.com/pinpoint/latest/userguide/welcome.html>.

Once the link is clicked, you will be notified that the email address has been verified.

## Congratulations!

You have successfully verified an email address. You can now start sending email from this address.

**For new Amazon SES users**—If you have not yet applied for a sending limit increase, then you are still in the [sandbox environment](#), and you can only send email to addresses that have been verified. To verify a new email address or domain, see the **Identity Management** section of the [Amazon SES console](#).

To confirm this, go back to the **Verified identities** screen, and refresh the browser window.

The screenshot shows the Amazon SES console interface. At the top, the breadcrumb navigation reads "Amazon SES > Configuration: Verified identities > liams.fitness@gmail.com". Below this, the email address "liams.fitness@gmail.com" is displayed in large text. To the right of the email address are two buttons: "Delete" and "Send test email".

Below the email address is a light blue informational box titled "Legacy TXT records" with an information icon. The text inside explains that domain verification is now based on DKIM and provides instructions on how to access legacy TXT records as a CSV file.

Below the informational box is a section titled "Summary for liams.fitness@gmail.com". This section contains a table with three columns: "Identity status", "Amazon Resource Name (ARN)", and "AWS Region".

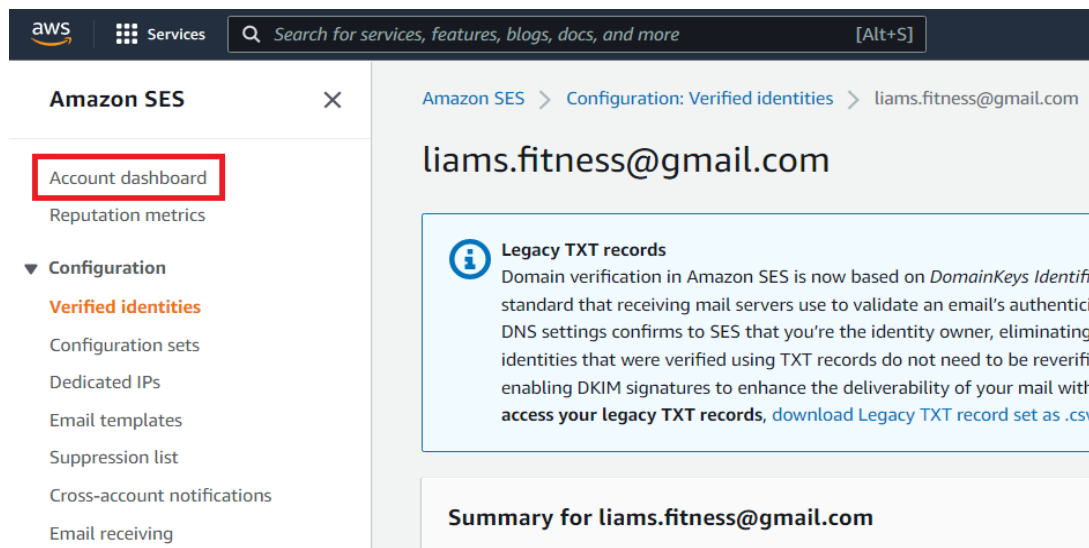
Identity status	Amazon Resource Name (ARN)	AWS Region
✓ Verified	arn:aws:ses:us-east-1:572092638768:identity/liams.fitness@gmail.com	US East (N. Virginia)

Next, we need to create SMTP credentials to access the Amazon SES SMTP interface.

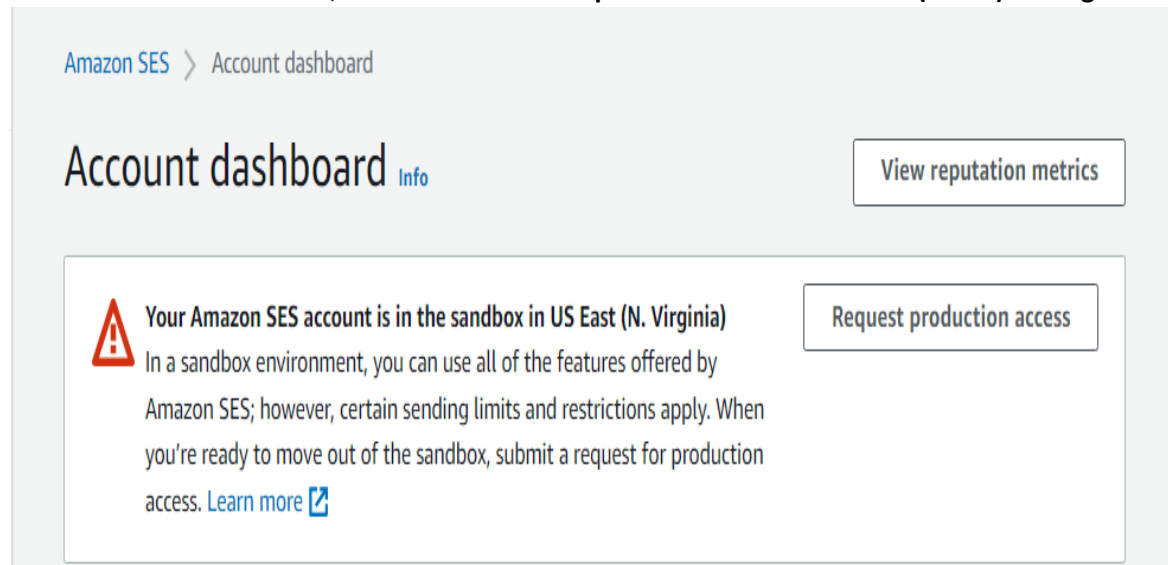
## Create SMTP Credentials

To be able to access the Amazon SES SMTP interface, which is region specific, we need to create SMTP credentials. I am in the US East (N. Virginia) **us-east-1** region, so I will create SMTP credentials in that region to access that region's SES SMTP interface (endpoint). While creating SMTP credentials an IAM (Identity & Access Management) user is created with privileges to access the SMTP interface and send emails.

On the left-hand side of the screen, under **Amazon SES**, click **Account Dashboard**



On the Account Dashboard, scroll down until **Simple Mail Transfer Protocol (SMTP) settings**



Then click **Create SMTP credentials**

### Simple Mail Transfer Protocol (SMTP) settings

You can use an SMTP-enabled programming language, email server, or application to connect to the Amazon SES SMTP interface. You'll need the following information and a set of SMTP credentials to configure this email sending method in US East (N. Virginia).

SMTP endpoint

email-smtp.us-east-1.amazonaws.com

STARTTLS Port

25, 587 or 2587

Transport Layer Security (TLS)

Required

TLS Wrapper Port

465 or 2465

### Authentication

You must have an Amazon SES SMTP user name and password to access the SMTP interface. These credentials are different from your AWS access keys and are unique to each region. To manage existing SMTP credentials, [visit the IAM console](#).

Create SMTP credentials

On the **Create User for SMTP** screen, enter an IAM User Name and click **Create**

This form lets you create an IAM user for SMTP authentication with Amazon SES. Enter the name of a new IAM user or accept the default and click Create to set up your SMTP credentials.

IAM User Name:

ses-smtp-user

Maximum 64 characters

[Show More Information](#)

Cancel


Create

Now click **Download Credentials** (credentials.csv). After the file is downloaded, click **Close**.

☒ Your 1 User(s) have been created successfully.

This is the only time these SMTP security credentials will be available for download. Credentials for SMTP users are only available when creating the user. For your protection, you should never share your SMTP credentials with anyone.

▼ Hide User SMTP Security Credentials

 <b>ses-smtp-user</b>	
SMTP Username:	AKIAYKM3A4YYIRWYC7JL
SMTP Password:	BFMyGjIh3Kmd+YYCqwMV6WPSiQyXb6X1eD6pGrakSNB6

Close **Download Credentials**

We will need the SMTP credentials when configuring an EC2 instance to send email.

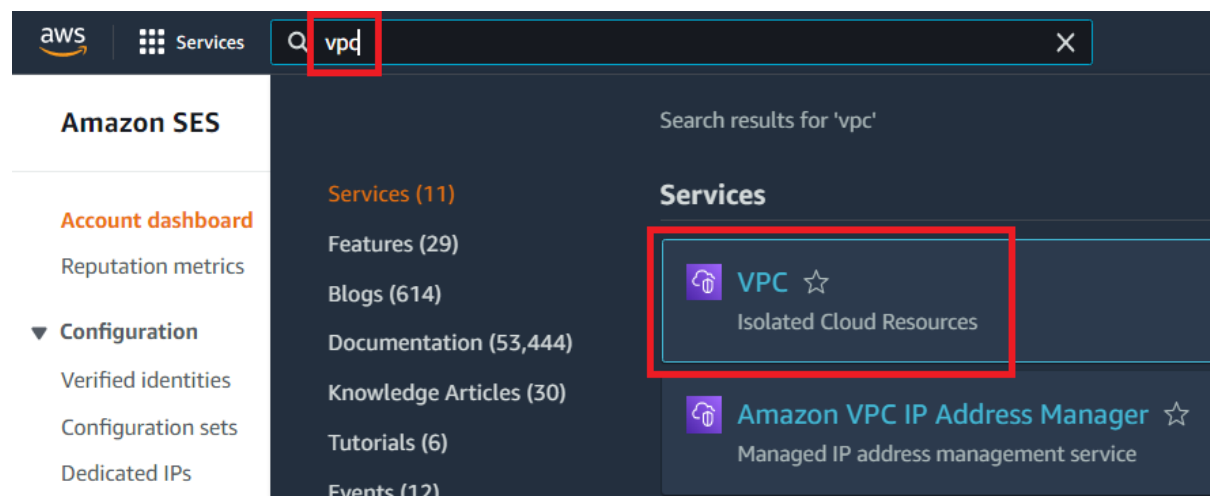
We have a verified identity and SMTP credentials. We are now ready to connect our EC2 instances to the Amazon SES service using a VPC Endpoint.

## Create VPC Endpoint

To allow our EC2 instances to send emails via Amazon SES, we need to create a VPC Endpoint which provides access to the Amazon SES SMTP interface.

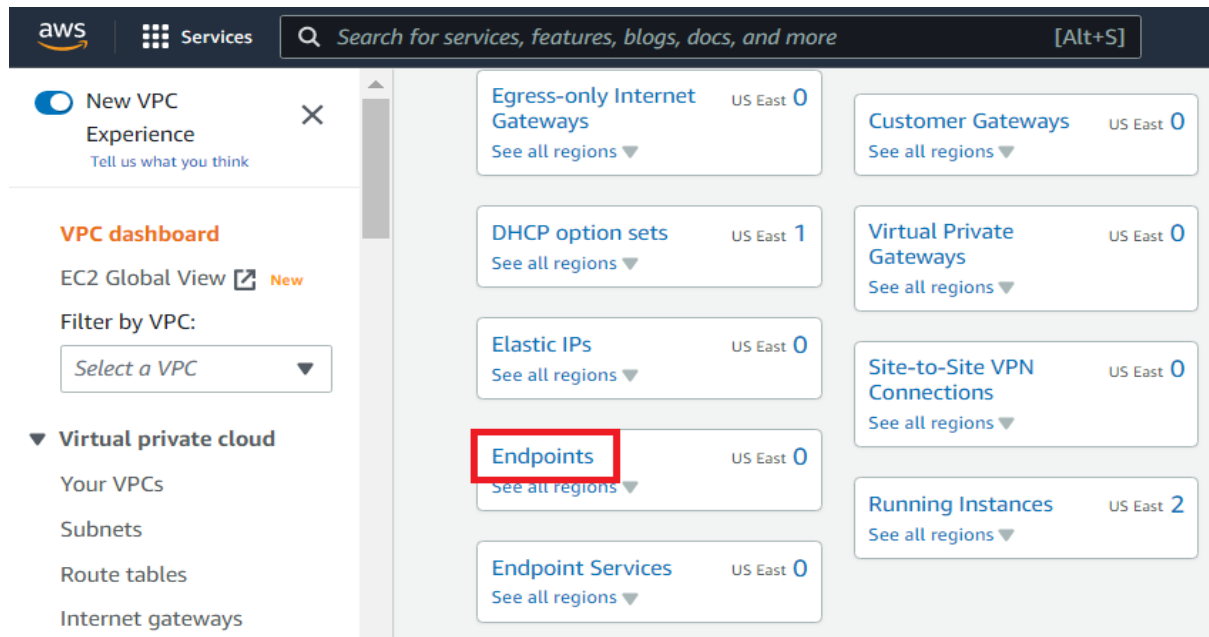
VPC Endpoint creation involves a few steps. First, identify the private IP address of the EC2 instances. In my case, I am using the entire subnet so that both of my instances will have access. Second, add an inbound rule to communicate with SMTP port (587). Third, create the VPC endpoint for the Amazon SES service.

In the search bar, enter **vpc** and select **VPC Isolated Cloud Resources**.

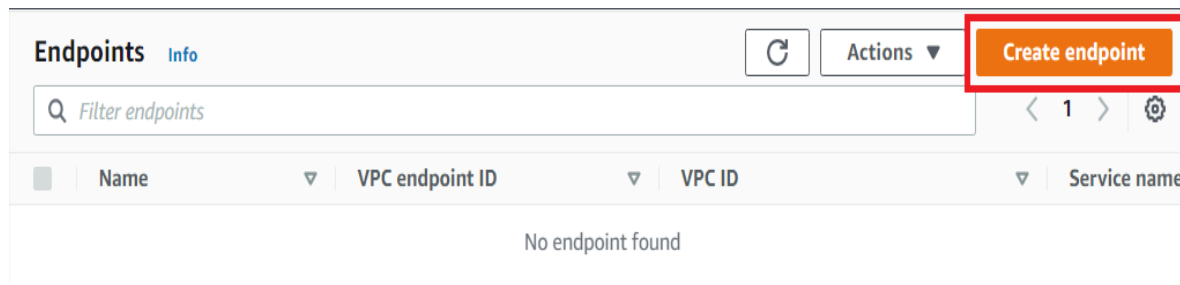


The screenshot shows the AWS Management Console search results for 'vpc'. The search bar at the top contains 'vpc'. On the left, the 'Amazon SES' sidebar is visible with links to 'Account dashboard', 'Reputation metrics', and 'Configuration'. The main content area shows 'Search results for 'vpc'' with a list of services. The 'VPC' service, described as 'Isolated Cloud Resources', is highlighted with a red box. Below it, 'Amazon VPC IP Address Manager' is also visible.

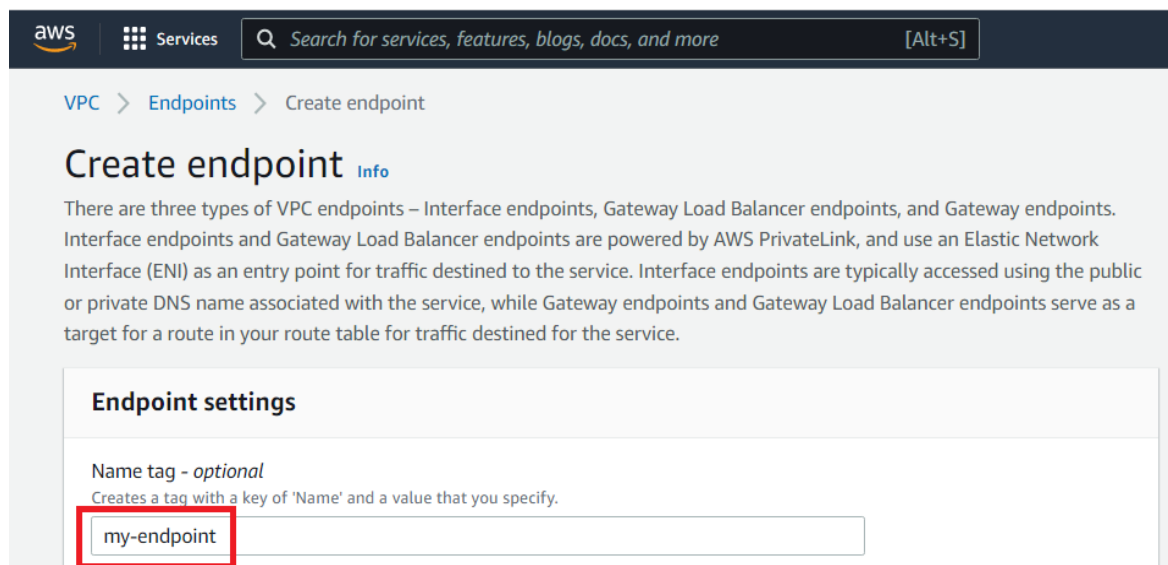
On the **VPC Dashboard**, scroll down and click **Endpoints**



On the **Endpoints** screen, click **Create Endpoint**



On the **Create Endpoint** screen, you can give it a name (optional)



Next, scroll down to the **Service Category** section and select **AWS Services**

### Service category

Select the service category

☒ **AWS services**  
Services provided by Amazon

☐ PrivateLink Ready partner services  
Services with an AWS Service Ready designation

☐ AWS Marketplace services  
Services that you've purchased through AWS Marketplace

☐ Other endpoint services  
Find services shared with you by service name

Under **Services**, enter **email** in the search box and choose the **Service Name: email-smtp**. You will notice that the service is region specific. In my case, I am in **us-east-1** (N.Virginia).

**Services (185)** 🔄

✕ < 1 2 3 4 5 6 7 ... 19 > ⚙️

**Service Name: com.amazonaws.us-east-1.email-smtp** ✕

aws.sagemaker.us-east-1.notebook amazon

Type

Interface

**Services (1/1)** 🔄

< 1 > ⚙️

**Service Name: com.amazonaws.us-east-1.email-smtp** ✕

Clear filters

Service Name	Owner	Type
<input checked="" type="radio"/> com.amazonaws.us-east-1.email-smtp	amazon	Interface

Under **VPC**, select the VPC you wish to use.

**VPC**  
Select the VPC in which to create the endpoint

**VPC**  
The VPC in which to create your endpoint.

▼ 🔄

**▶ Additional settings**



Under Subnets, choose the subnet you wish to use. For me, I will choose the subnet & availability zone (gathered earlier in the tutorial) that my EC2 instances use.

**Subnets ( 1/3 )** [Info](#)

<input type="checkbox"/>	Availability Zone	Subnet ID
<input type="checkbox"/>	us-east-1a (use1-az6)	
<input checked="" type="checkbox"/>	us-east-1b (use1-az1)	subnet-0096efb1b7740b3da
<input type="checkbox"/>	us-east-1d (use1-az4)	

subnet-0096efb1b7740b3da

subnet\_default

IP address type

☒ IPv4

☐ IPv6

☐ Dualstack

Under **Security Groups**, I have chosen **security-group1** used by both of my EC2 instances.

**Security groups (1/3)** [Info](#)

1

<input type="checkbox"/>	Group ID	Group name	VPC ID
<input checked="" type="checkbox"/>	sg-02520767438262038	security-group1	vpc-01ac0d160f388
<input type="checkbox"/>	sg-07d39b68f2403b7c8	default	vpc-01ac0d160f388
<input type="checkbox"/>	sg-0a1d0061cebed314b	security-group2	vpc-01ac0d160f388

sg-02520767438262038

Finally, click **Create endpoint**

**Tags**

Key

Value - optional

You can add 49 more tags.

The VPC Endpoint has been created for the Amazon SES SMTP interface.

Endpoints (1) <a href="#">Info</a>					<a href="#">Refresh</a>	<a href="#">Actions</a>	<a href="#">Create endpoint</a>
<input type="text" value="Filter endpoints"/>					< 1 > <a href="#">Settings</a>		
<input type="checkbox"/>	Name	VPC endpoint ID	VPC ID	Service name			
<input type="checkbox"/>	my-endpoint	vpce-084c597f563d15cca	vpce-01ac0d160f388c36e   vpc_default	com.amazonaws.us-east-1.email-smtp			

I will now return to the Amazon SES console and use the mailbox simulator to send a test email.

## Simple Email Service Test

Back on the **Amazon SES Account dashboard**, ensure **Verified identities** is selected and click on the email address that is a verified identity.

aws

Services

[Alt+S]

N. Virginia

liamsfitness

Amazon SES

Account dashboard

Reputation metrics

Configuration

Verified identities

Configuration sets

Dedicated IPs

Email templates

Suppression list

Cross-account notifications

Email receiving

Amazon SES > Configuration: Verified identities

Verified identities

A verified identity is a domain, subdomain, or email address you use to send email through Amazon SES. [Learn more](#)

**New identity status update**  
The **Identity status** now represents the explicit verification of the identity itself. For the domain identities this means verifying ownership through updates in the DNS records, and for the email address identities, this means opening the verification email from `no-reply-aws@amazon.com` and selecting the link to complete the verification process. [Learn more](#)

Identities (1) [Info](#)

< 1 > [Settings](#)

<input type="checkbox"/>	Identity	Identity type	Identity status
<input type="checkbox"/>	liams.fitness@gmail.com	Email address	Verified

Feedback

Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)

[Terms](#)

[Cookie preferences](#)

Next, I will click on **Send test email**

The screenshot shows the Amazon SES console interface. On the left is a navigation menu with options like 'Account dashboard', 'Reputation metrics', 'Configuration', 'Verified identities', 'Configuration sets', 'Dedicated IPs', 'Email templates', 'Suppression list', 'Cross-account notifications', and 'Email receiving'. The main content area is titled 'liams.fitness@gmail.com' and includes a 'Delete' button and a 'Send test email' button, which is highlighted with a red rectangular box. Below this is an informational box about 'Legacy TXT records'. At the bottom, a 'Summary for liams.fitness@gmail.com' table shows the identity status as 'Verified', the Amazon Resource Name (ARN) as 'arn:aws:ses:us-east-1:572092638768:identity/liams.fitness@gmail.com', and the AWS Region as 'US East (N. Virginia)'.

Summary for liams.fitness@gmail.com		
Identity status	Amazon Resource Name (ARN)	AWS Region
Verified	arn:aws:ses:us-east-1:572092638768:identity/liams.fitness@gmail.com	US East (N. Virginia)

Remember that I am in the SES sandbox so I can only use my verified identity (email address) as both the sender and recipient of the test email.

On the **Send test email** screen, ensure the **Email format** selected is **Formatted** and that the **From-address** is a verified identity.

The screenshot shows the 'Send test email' screen in the Amazon SES console. The breadcrumb navigation at the top reads 'Amazon SES > Configuration: Verified identities > liams.fitness@gmail.com > Send test email'. The main heading is 'Send test email' with an 'Info' link. Below this is a descriptive paragraph about the mailbox simulator. The 'Message details' section contains two radio button options for 'Email format': 'Formatted' (selected and highlighted with a red box) and 'Raw'. The 'From-address' field is also highlighted with a red box and contains the text 'liams.fitness@gmail.com'.

Then, scroll down the page and set **Scenario** to **Custom**, **Custom recipient** to a verified identity, a subject and, optionally, an email body. Leave **Configuration set** unselected, as it is also optional.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Scenario [Info](#)

Choose the email sending scenario that you want to simulate. Each scenario corresponds to a different recipient email address managed by the mailbox simulator. To specify a custom recipient, select Custom.

Custom  
Use a recipient address of your own

Custom recipient

While your account is in the Amazon SES sandbox, you can only send test emails to other verified identities. If you've verified an identity at the domain level, you can send a test email to any email address under that verified domain.

liams.fitness@gmail.com

Subject

Amazon SES Test Email #1

Body - optional

This email was sent using the Amazon SES mailbox simulator

Configuration set - optional [Info](#)

Choose a configuration set

Feedback Looking for language selection? Find it in the new [Unified Settings](#) © 2022, Amazon Web Services

Then, scroll down to the bottom of the page and click **Send test email**

Body - optional

This email was sent using the Amazon SES mailbox simulator

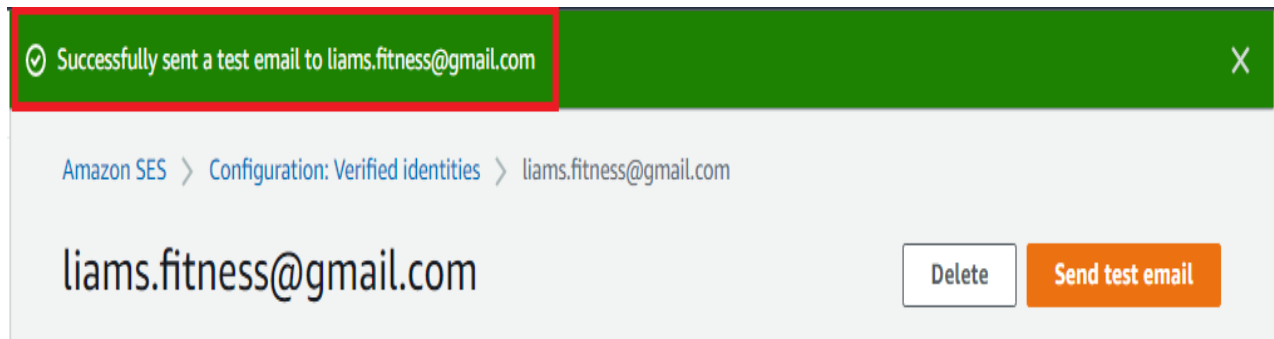
Configuration set - optional [Info](#)

Choose a configuration set

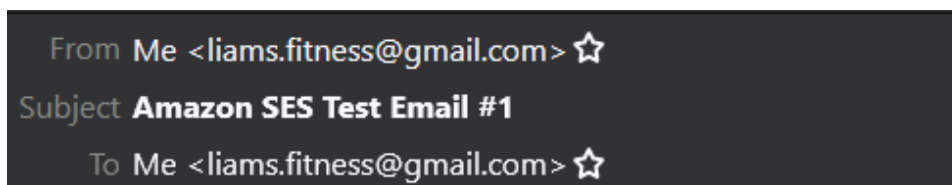
► Additional configurations- optional

Cancel Send test email

Back on the **Amazon SES console** screen, I see the successful notification about test email transmission.



I can confirm receipt by checking my email client:



This email was sent using the Amazon SES mailbox simulator

I hope you've enjoyed this tutorial.

We successfully configured the components required by Amazon SES (Simple Email Service):

- A verified identity (email address)
- SMTP credentials to access the Amazon SES SMTP interface
- VPC endpoint provides access to the Amazon SES SMTP interface
- EC2 instance details for VPC endpoint:
  - security group, subnet & availability zone
- Inbound Rule for port 587 added to security group to allow email transmission

Finally, we validated the configured components by successfully sending a test email using the Amazon SES mailbox simulator.

Now that Amazon SES is ready to use, you will want to see my Postfix tutorials where I demonstrate the installation, and configuration, of Postfix as an outbound send-only email server, on an Ubuntu 20 EC2 & RHEL 8 EC2. These tutorials include how to send emails manually using **sendmail** and automatically using **cron jobs**; both via Amazon SES.

The **AWS Ubuntu 20 EC2 Postfix Install** tutorial is accessible [here](#), while the **AWS RHEL 8 EC2 Postfix Install** tutorial is accessible [here](#). My main tutorials page is accessible [here](#).

Please be aware of the charges of \$0.01 per VPC endpoint hour & \$0.01 per GB for up to 1 PB monthly data processed. Although you, most likely, won't be charged for data processing, you will be charged \$0.01 for every hour the VPC endpoint is active.

[Back to Top](#)