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.

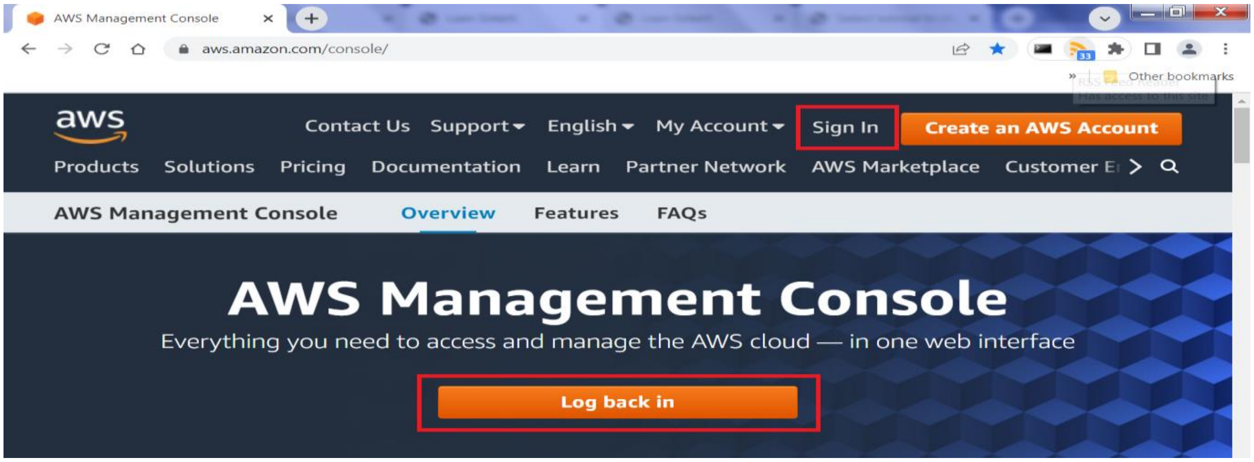
After completing this tutorial, you will be ready for my Postfix tutorials where I demonstrate the installation, and configuration, of Postfix as an outbound send-only email server, on an Ubuntu 20 EC2 & RHEL 8 EC2. Postfix will allow you to fully utilize Amazon SES.

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
- Simple Email Service Test

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



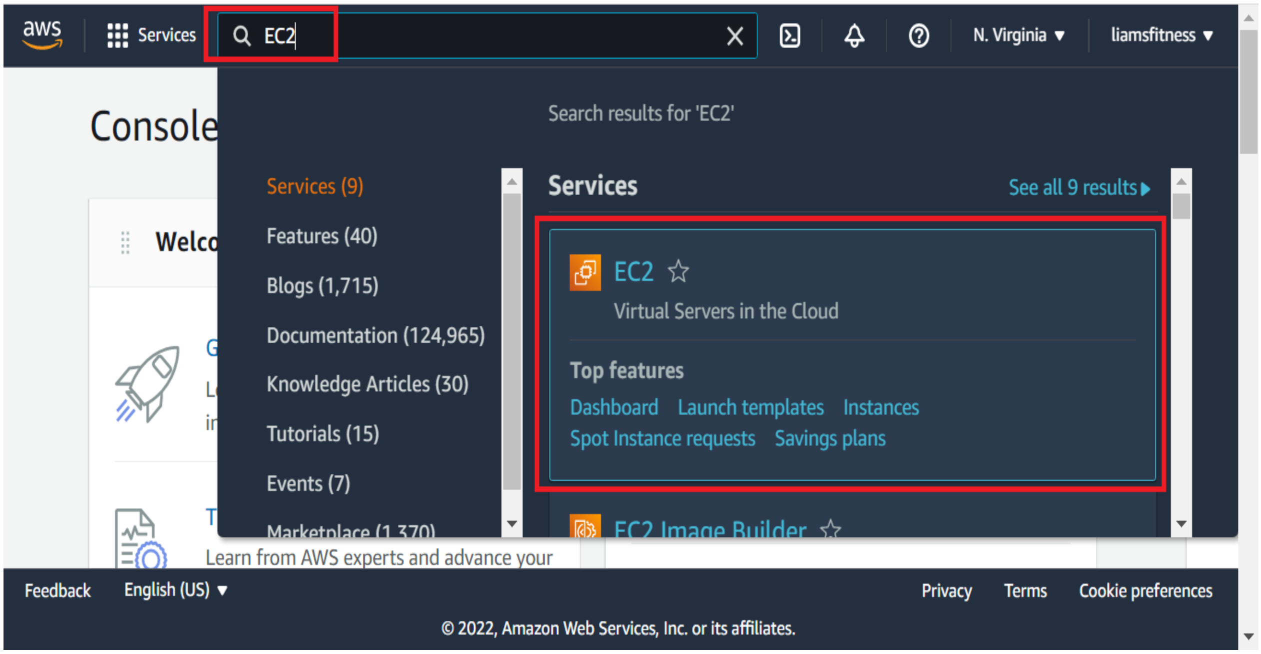
AWS Management Console

Everything you need to access and manage the AWS cloud — in one web interface

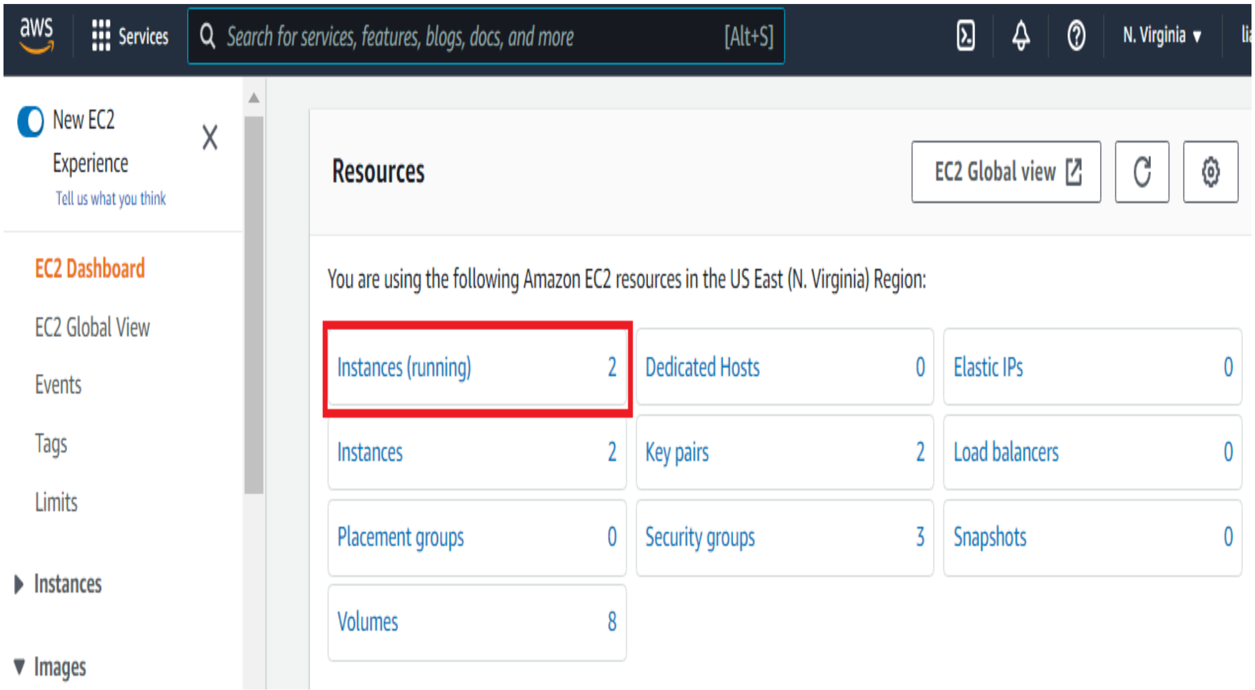
Before we configure the Amazon Simple Email Service, I will first gather the necessary information from both my EC2 instances: **security group** & **subnet**. Both of these values will be used when adding a new inbound rule to the security group.

Gather EC2 Instance Information

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



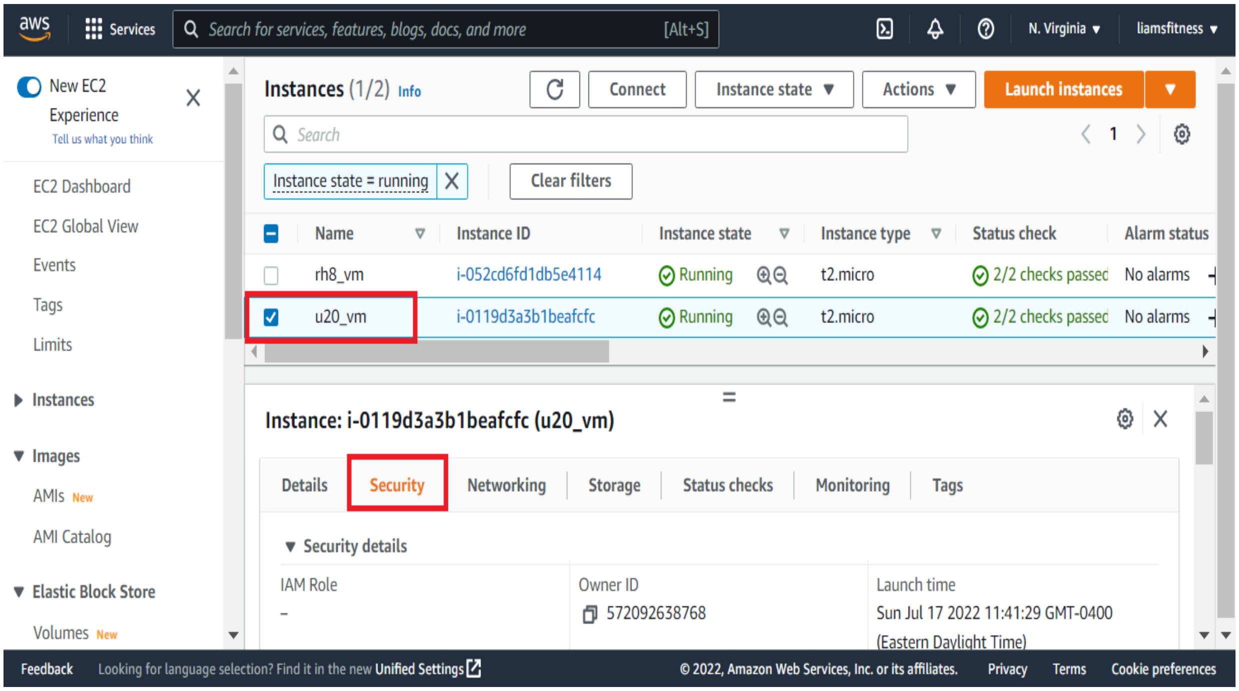
On the EC2 Dashboard, select **Instances (running)**



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

Instances (running)	2	Dedicated Hosts	0	Elastic IPs	0
Instances	2	Key pairs	2	Load balancers	0
Placement groups	0	Security groups	3	Snapshots	0
Volumes	8				

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**).

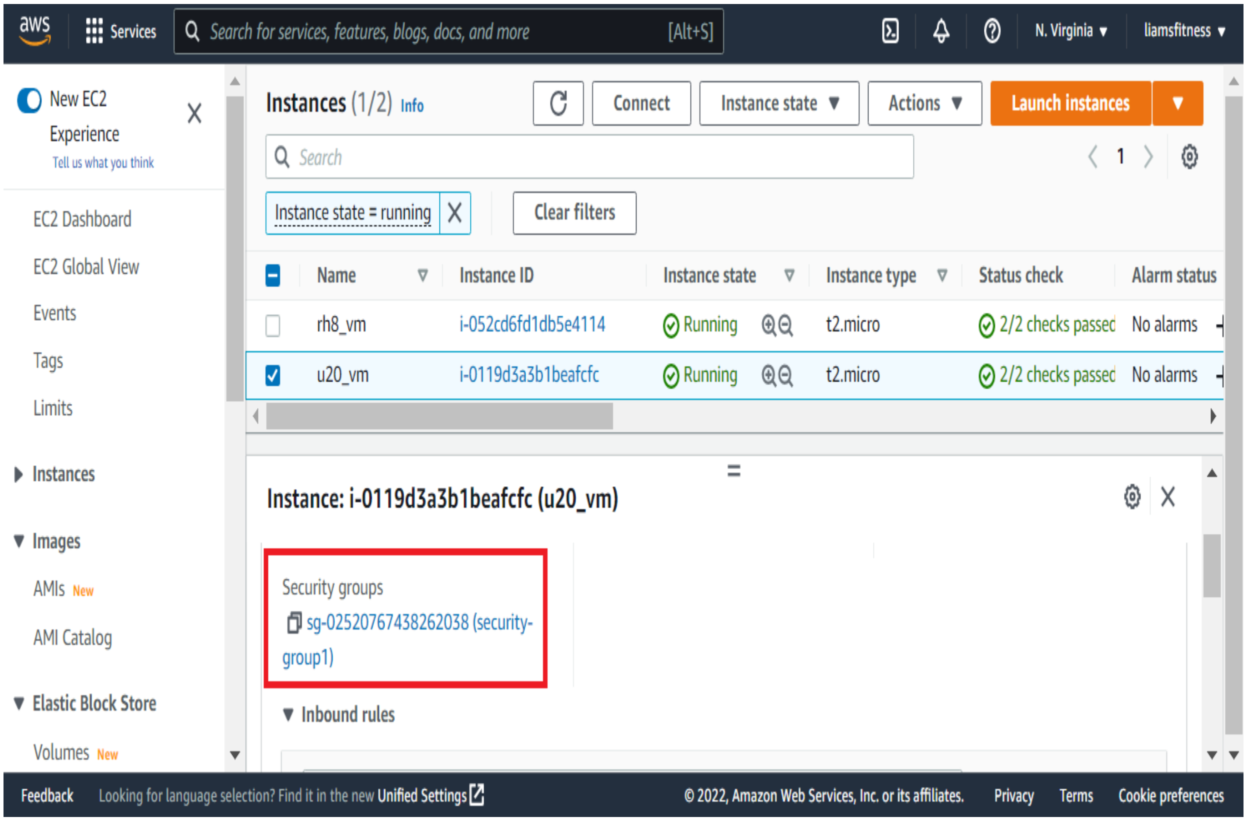


	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
☑	u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-0119d3a3b1beafcfc (u20_vm)

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**.

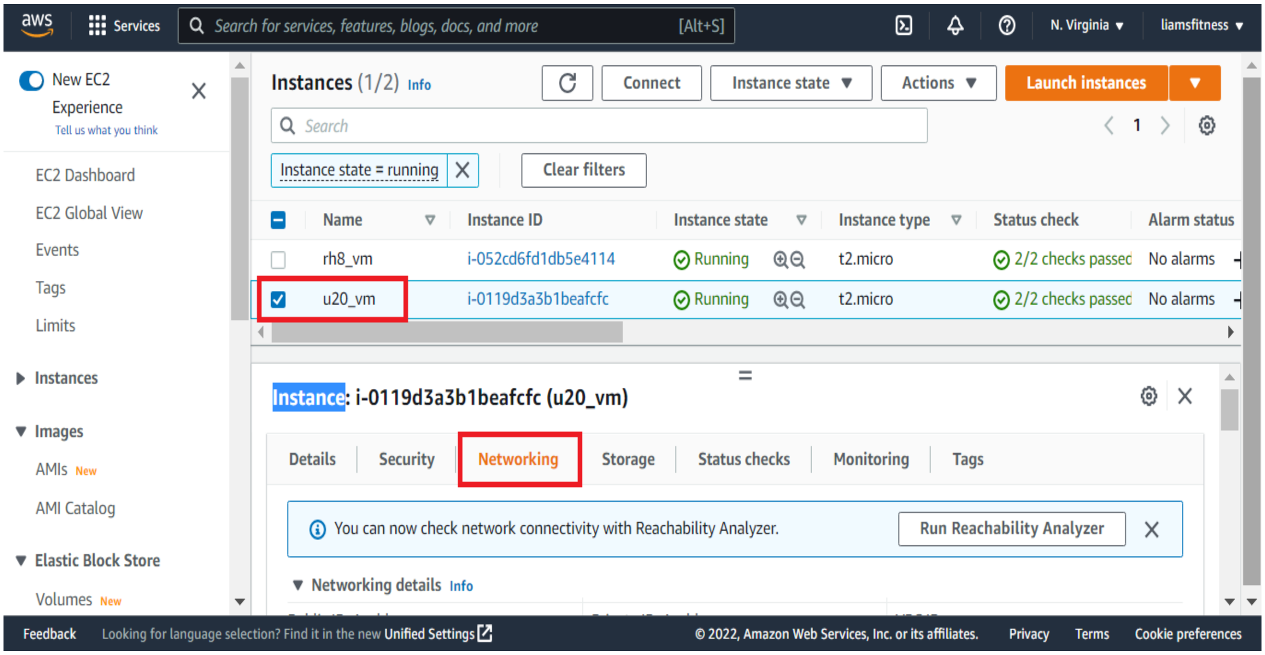


	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
☑	u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-0119d3a3b1beafcfc (u20_vm)

Security groups
sg-02520767438262038 (security-group1)

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

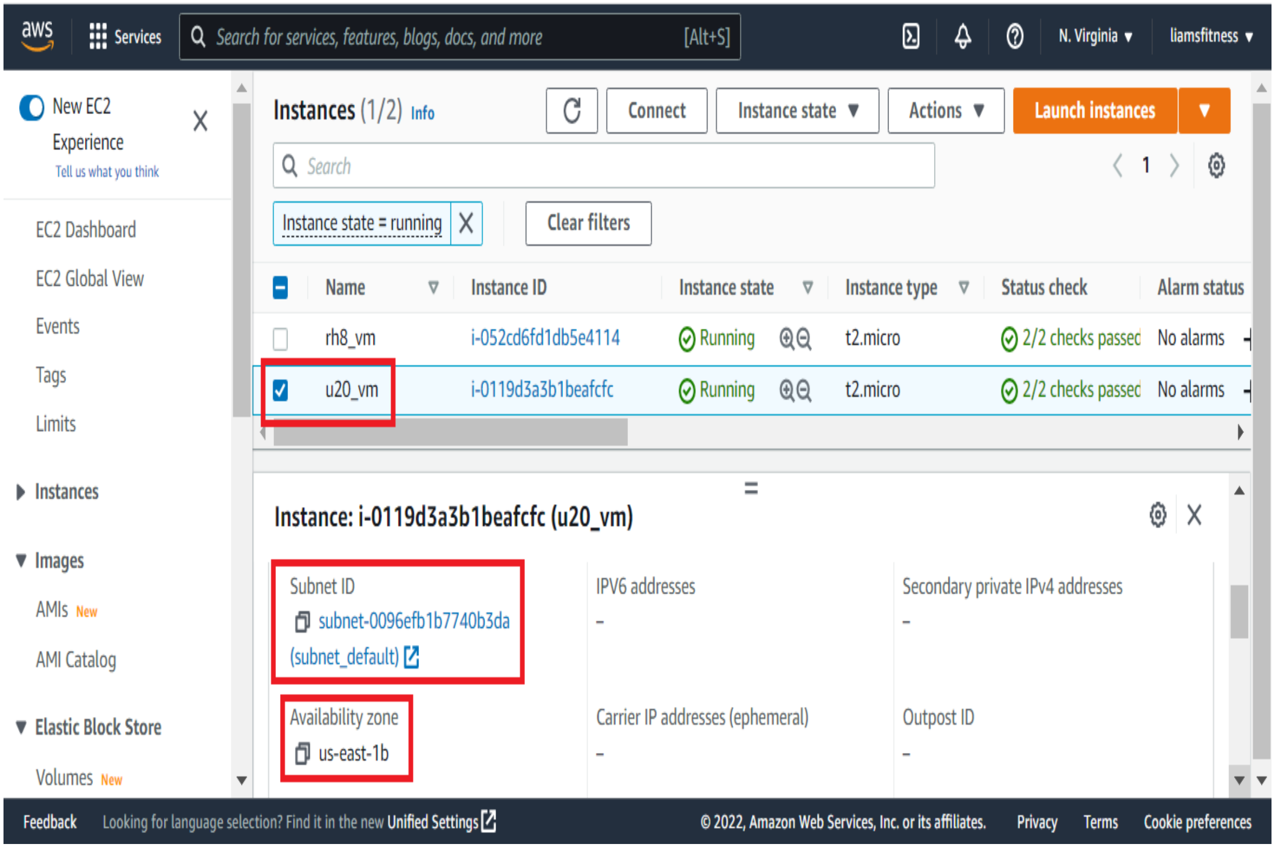


	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
☑	u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-0119d3a3b1beafcfc (u20_vm)

You can now check network connectivity with Reachability Analyzer.

In the bottom section of the screen, under the **Networking** tab, scroll down until **Subnet ID** is visible and note the value. In my case the value is **subnet_default**



	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)

Subnet ID
subnet-0096efb1b7740b3da (subnet_default)

IPV6 addresses
–

Secondary private IPv4 addresses
–

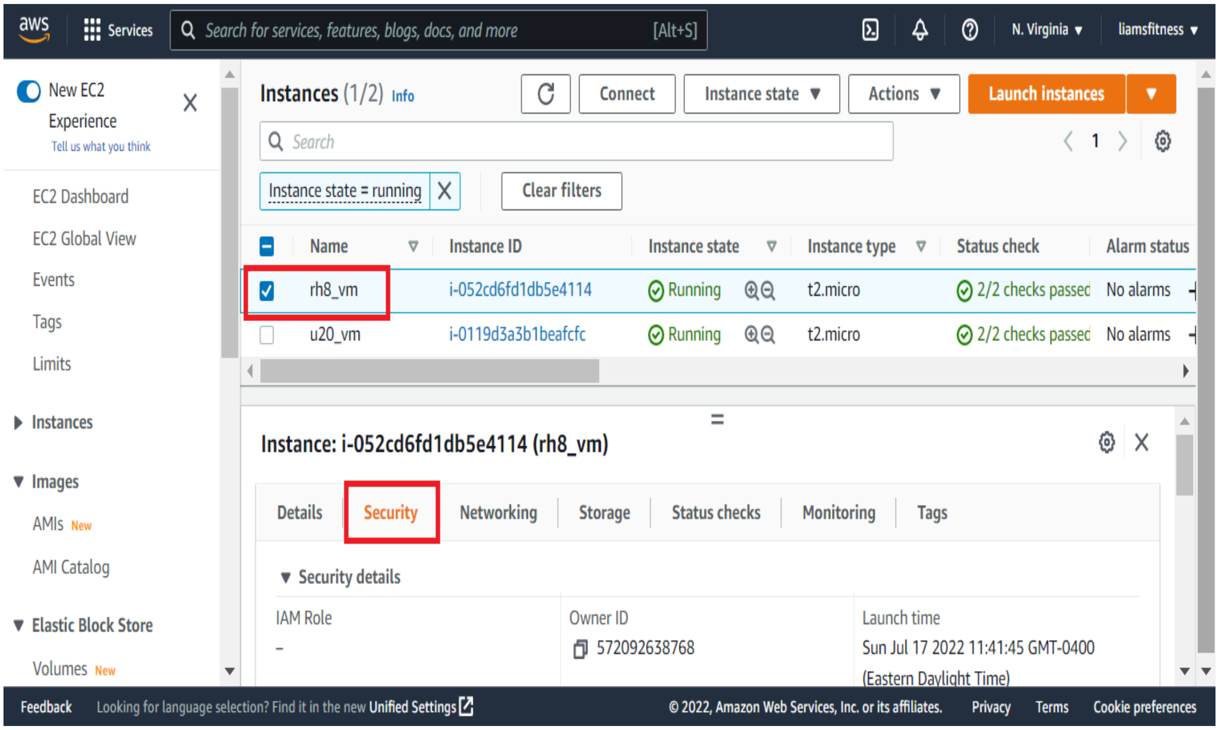
Availability zone
us-east-1b

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.



Instances (1/2) Info

Instance state = running ☒

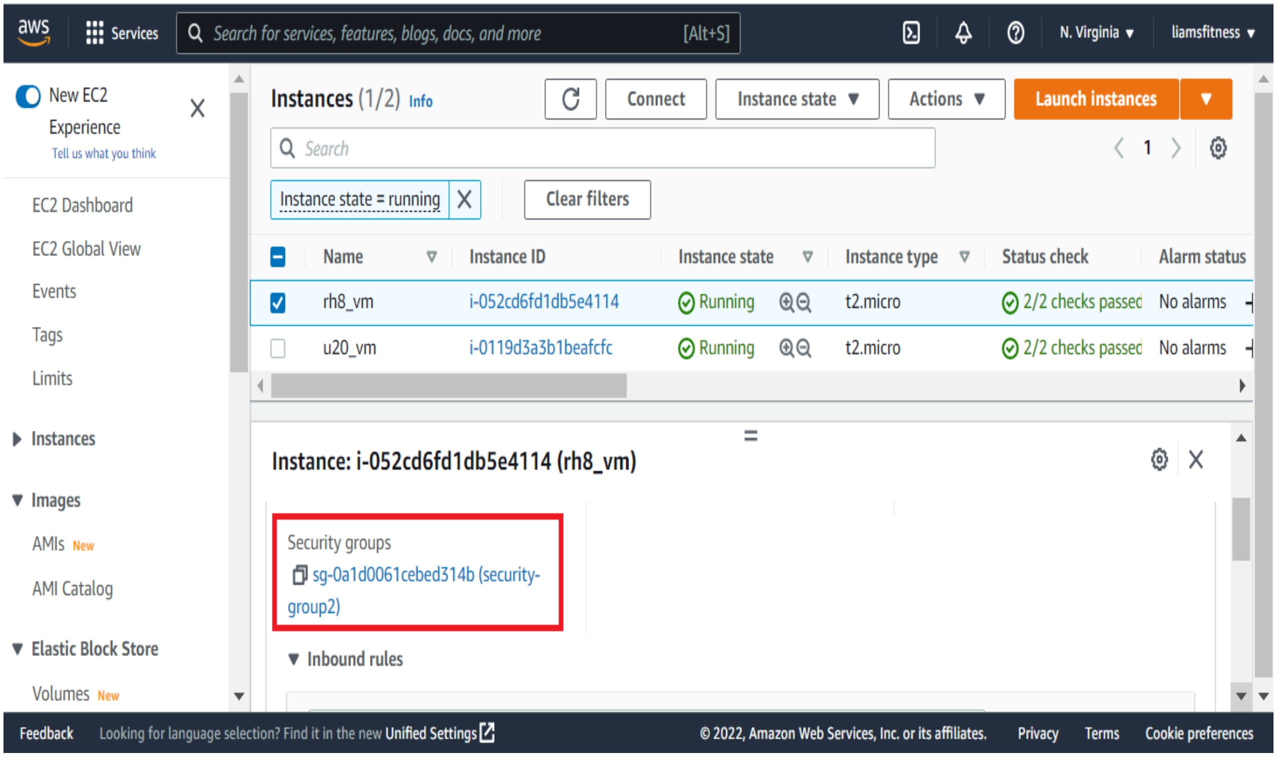
▬	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	rh8_vm	i-052cd6fd1db5e4114	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms
□	u20_vm	i-0119d3a3b1beafcfc	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms

Instance: i-052cd6fd1db5e4114 (rh8_vm)

▾ 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**.



Instances (1/2) Info

Instance state = running ☒

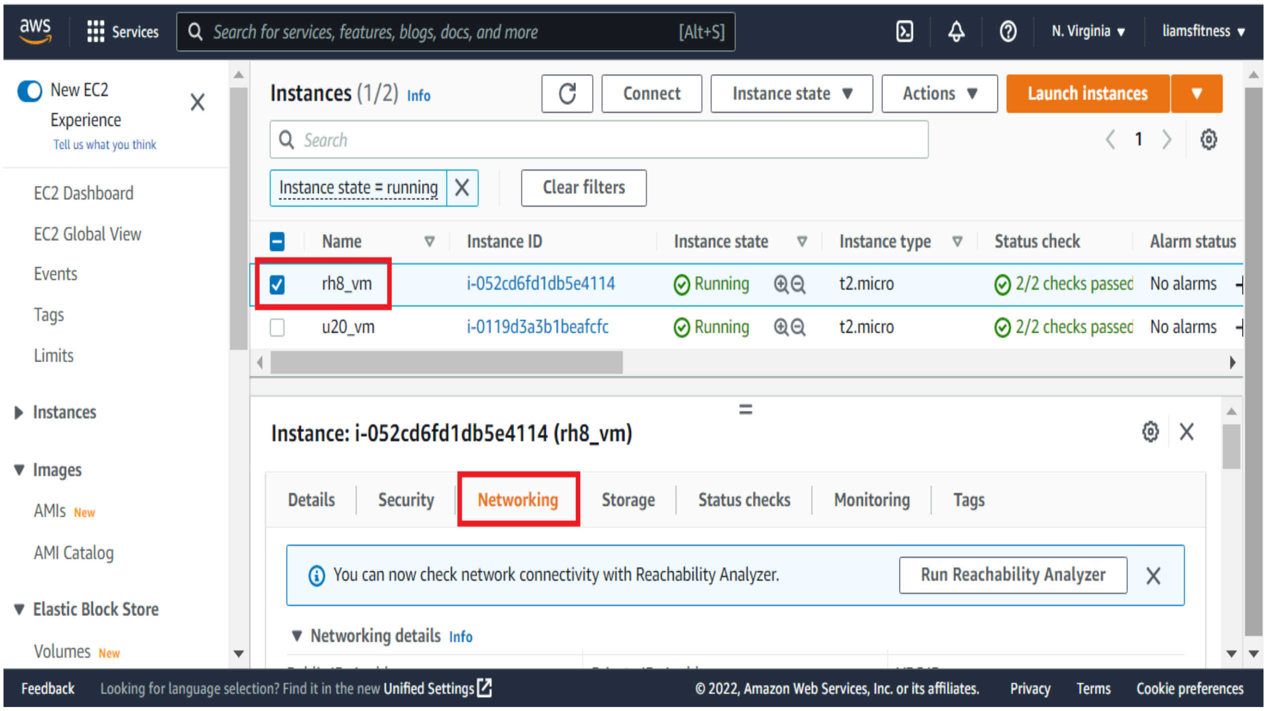
▬	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	rh8_vm	i-052cd6fd1db5e4114	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms
□	u20_vm	i-0119d3a3b1beafcfc	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms

Instance: i-052cd6fd1db5e4114 (rh8_vm)

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.



Instances (1/2) Info

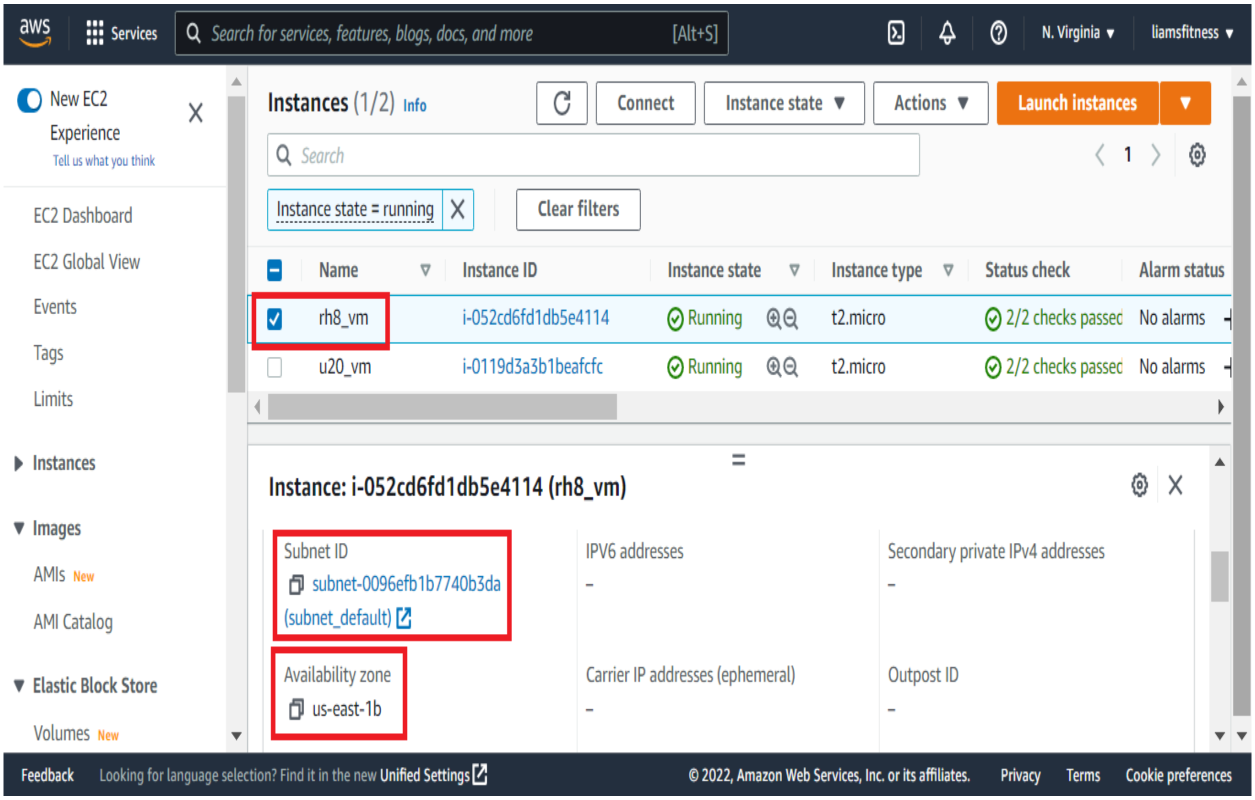
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
☑	rh8_vm	i-052cd6fd1db5e4114	Running	t2.micro	2/2 checks passed	No alarms
□	u20_vm	i-0119d3a3b1beafcfc	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-052cd6fd1db5e4114 (rh8_vm)

You can now check network connectivity with Reachability Analyzer.

▼ Networking details Info

In the bottom section of the screen, under the **Networking** tab, scroll down until **Subnet ID** is visible and note the value. In my case the value is **subnet_default**



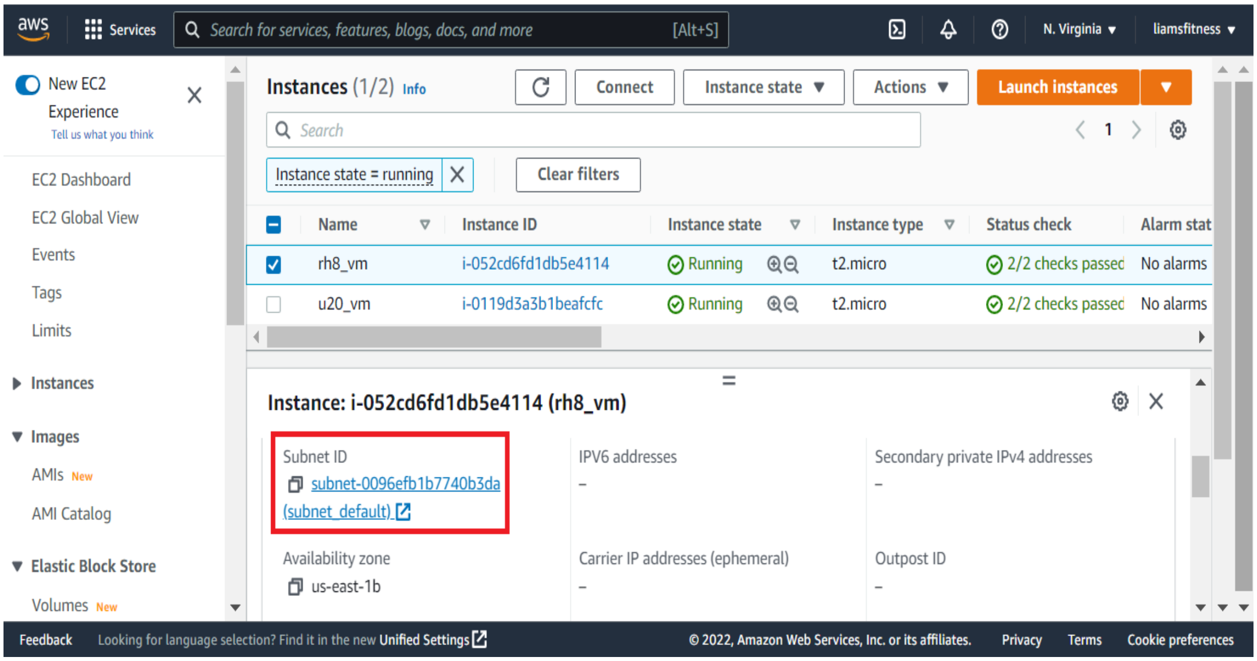
Instances (1/2) Info

	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)

Subnet ID subnet-0096efb1b7740b3da (subnet_default)	IPV6 addresses –	Secondary private IPv4 addresses –
Availability zone us-east-1b	Carrier IP addresses (ephemeral) –	Outpost ID –

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**



Instances (1/2) Info

Instance state = running

	Name	Instance ID	Instance state	Instance type	Status check	Alarm stat
☑	rh8_vm	i-052cd6fd1db5e4114	✓ Running	t2.micro	✓ 2/2 checks passec	No alarms
□	u20_vm	i-0119d3a3b1beafcfc	✓ Running	t2.micro	✓ 2/2 checks passec	No alarms

Instance: i-052cd6fd1db5e4114 (rh8_vm)

Subnet ID
subnet-0096efb1b7740b3da (subnet_default)

IPV6 addresses
–

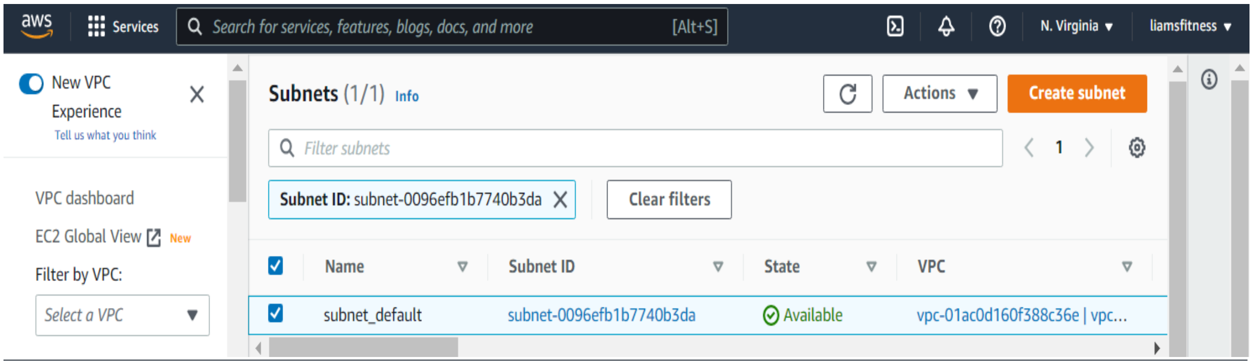
Secondary private IPv4 addresses
–

Availability zone
us-east-1b

Carrier IP addresses (ephemeral)
–

Outpost ID
–

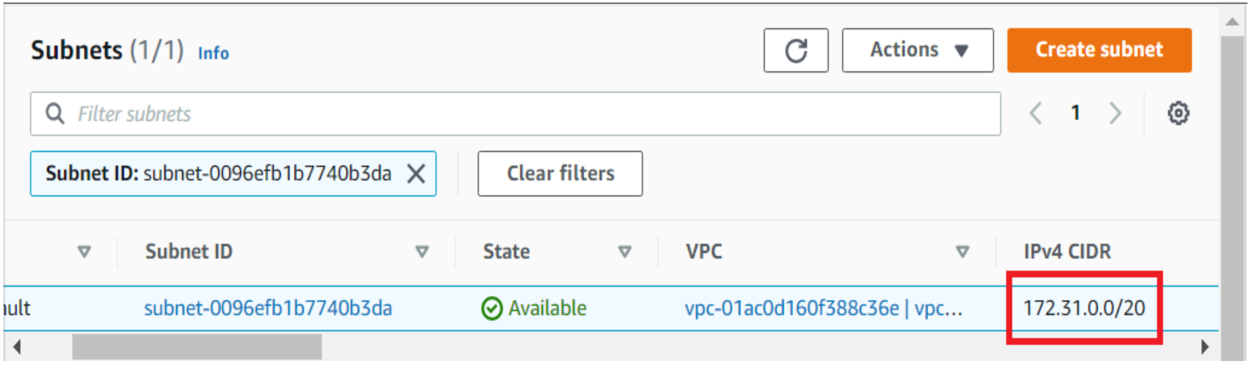
The **Subnets** screen will open in a new tab. On the **Subnets** screen, scroll to the right until the **IPv4 CIDR** heading is visible and note the value.



Subnets (1/1) Info

Subnet ID: subnet-0096efb1b7740b3da

☑	Name	Subnet ID	State	VPC
☑	subnet_default	subnet-0096efb1b7740b3da	✓ Available	vpc-01ac0d160f388c36e | vpc...



Subnets (1/1) Info

Subnet ID: subnet-0096efb1b7740b3da

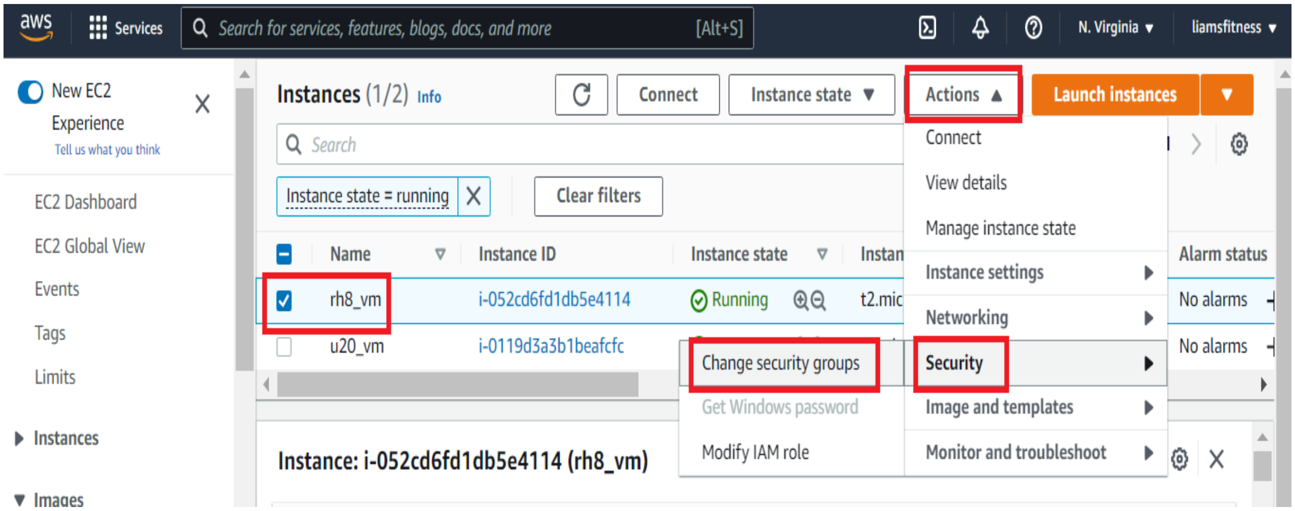
	Subnet ID	State	VPC	IPv4 CIDR
ult	subnet-0096efb1b7740b3da	✓ Available	vpc-01ac0d160f388c36e | vpc...	172.31.0.0/20

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.

Change EC2 Instance Security Group

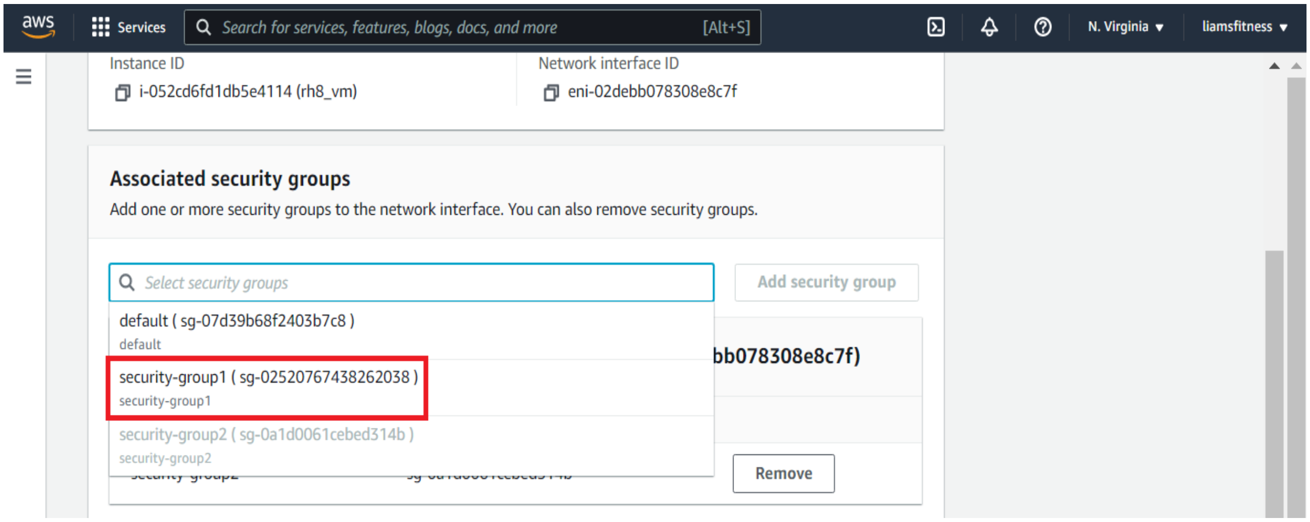
Back on the **Instances** screen, to change my RHEL 8 EC2 instance's security group, I will first ensure it is selected. Then, I will click the **Actions** menu, scroll down and click **Security** followed by **change security groups**.



	Name	Instance ID	Instance state	Instan	Alarm status
☑	rh8_vm	i-052cd6fd1db5e4114	Running	t2.mic	No alarms
□	u20_vm	i-0119d3a3b1beafcfc			No alarms

Instance: i-052cd6fd1db5e4114 (rh8_vm)

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**



Instance ID
i-052cd6fd1db5e4114 (rh8_vm)

Network interface ID
eni-02debb078308e8c7f

Associated security groups

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

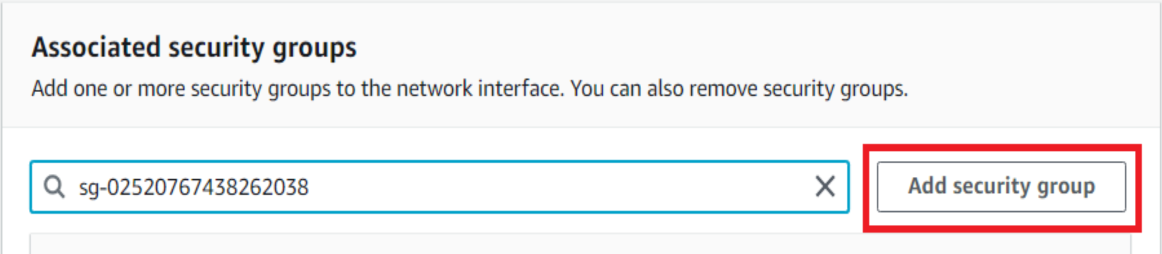
default (sg-07d39b68f2403b7c8)
default

security-group1 (sg-02520767438262038)
security-group1

security-group2 (sg-0a1d0061cebed314b)
security-group2

bb078308e8c7f)

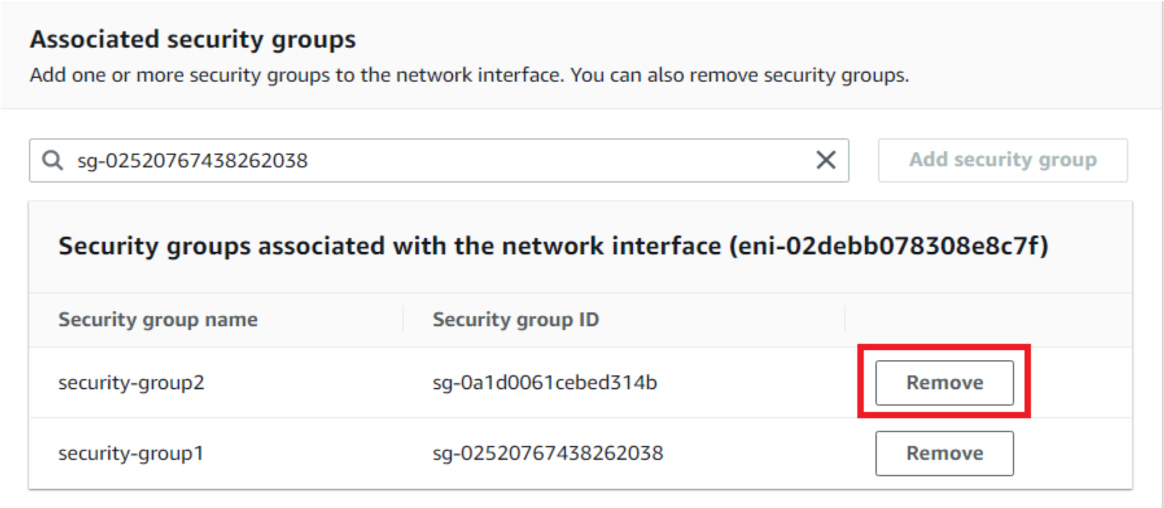
Next, click **Add security group**



Associated security groups

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

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



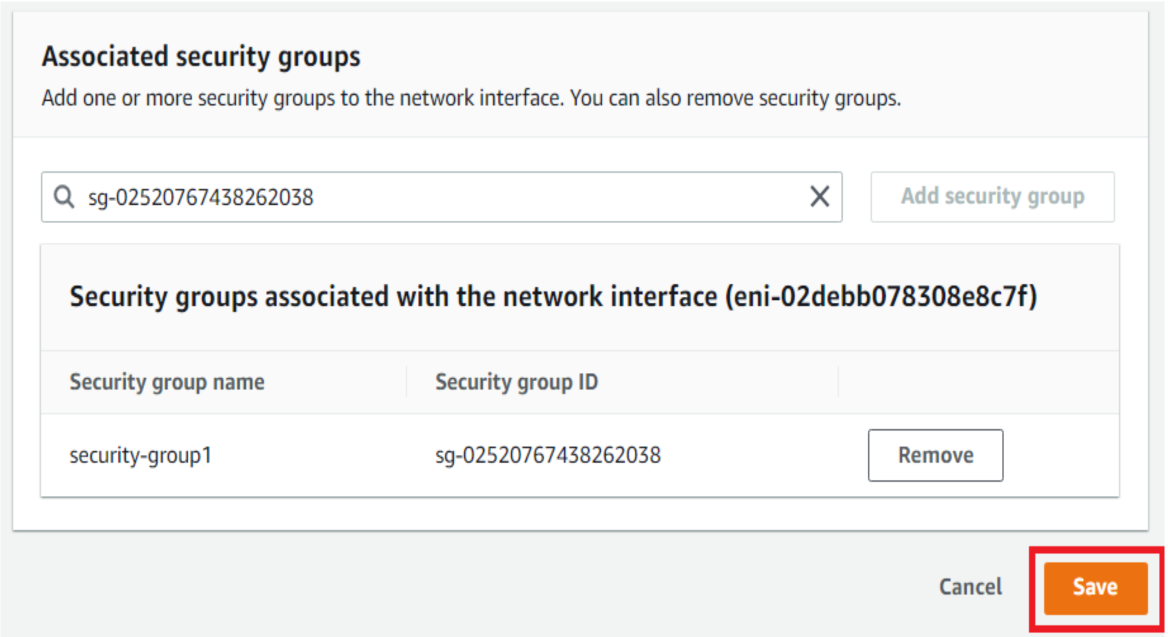
Associated security groups

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

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**

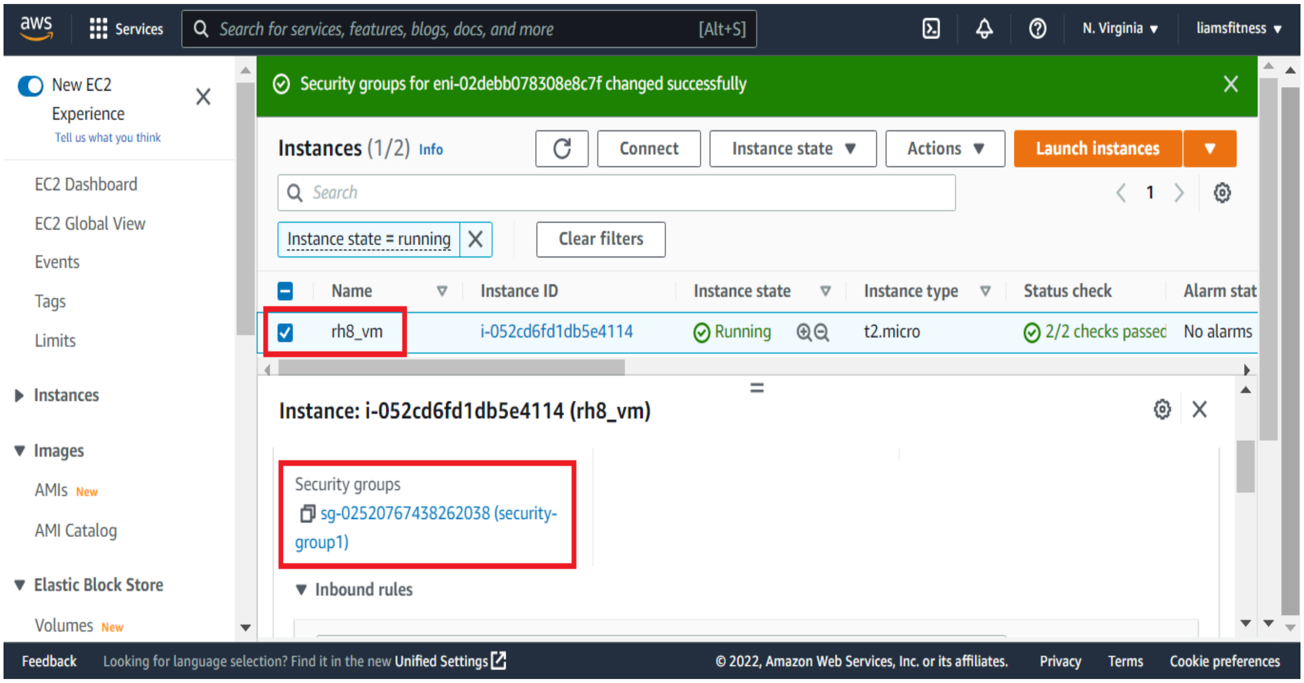


Associated security groups

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

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

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



Security groups for eni-02debb078308e8c7f changed successfully

Instances (1/2) Info

Instance state = running

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

Instance: i-052cd6fd1db5e4114 (rh8_vm)

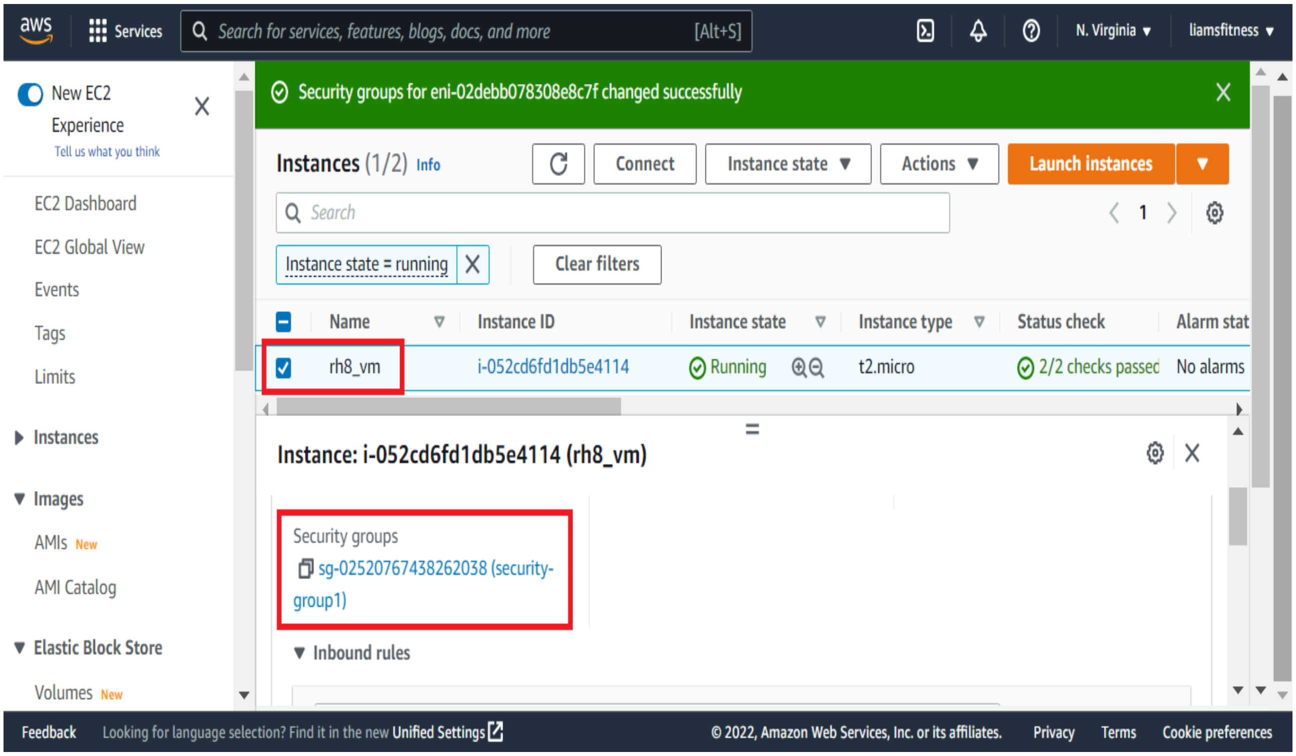
Security groups
sg-02520767438262038 (security-group1)

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**).



Security groups for eni-02debb078308e8c7f changed successfully

Instances (1/2) Info

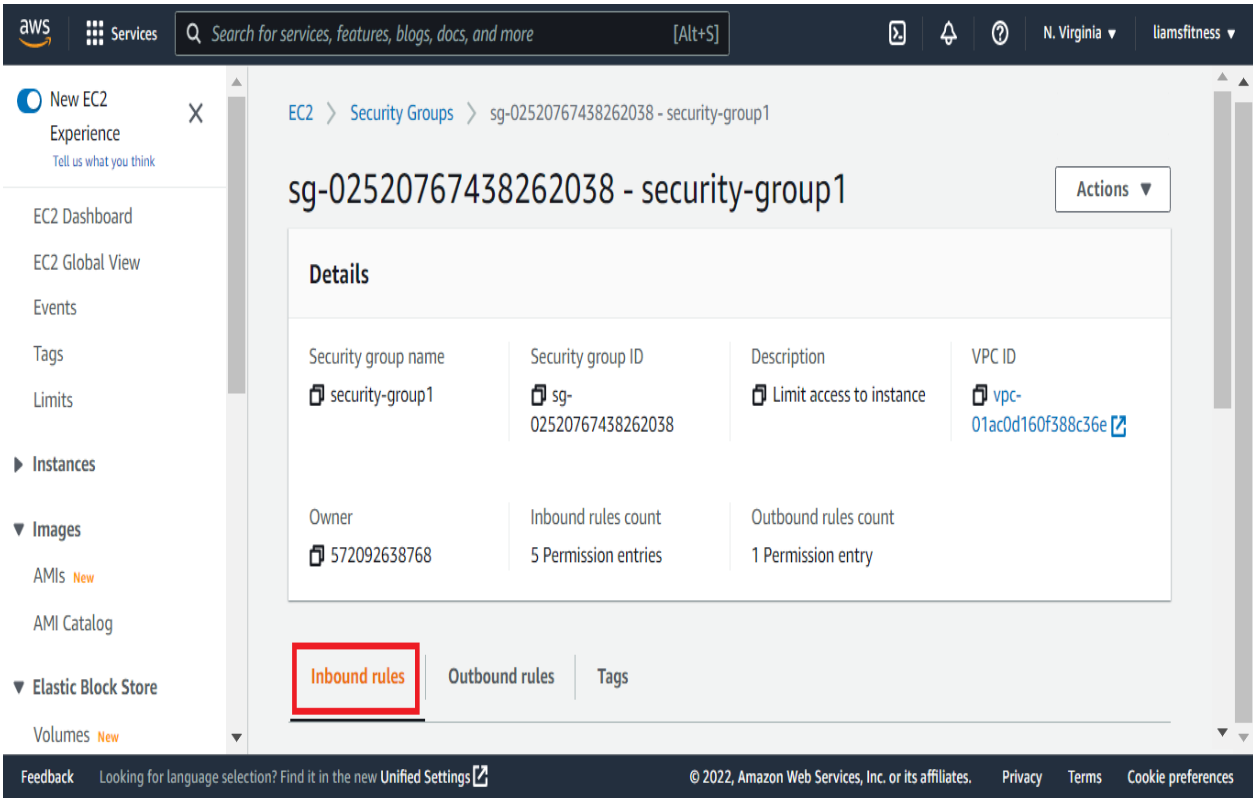
Instance state = running

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

Instance: i-052cd6fd1db5e4114 (rh8_vm)

Security groups
sg-02520767438262038 (security-group1)

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



sg-02520767438262038 - security-group1

Details

Security group name: security-group1

Security group ID: sg-02520767438262038

Description: Limit access to instance

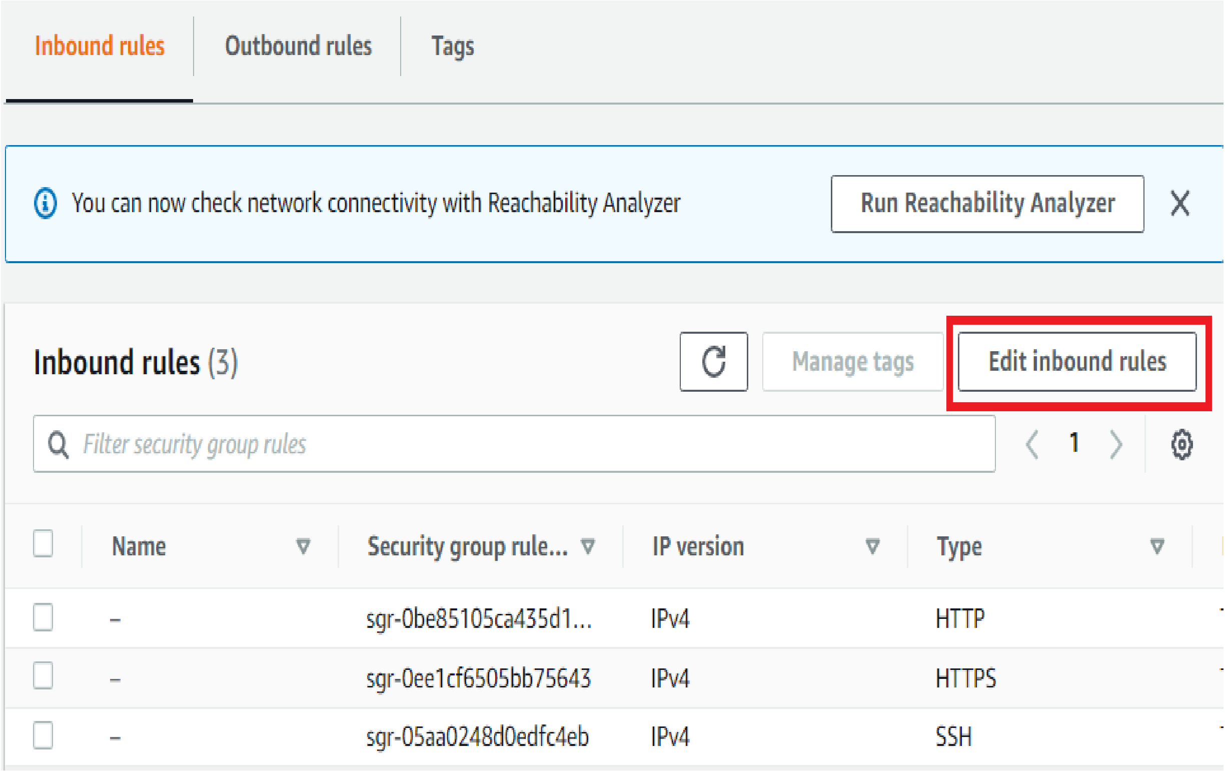
VPC ID: vpc-01ac0d160f388c36e

Owner: 572092638768

Inbound rules count: 5 Permission entries

Outbound rules count: 1 Permission entry

Next, click **Edit Inbound Rules**

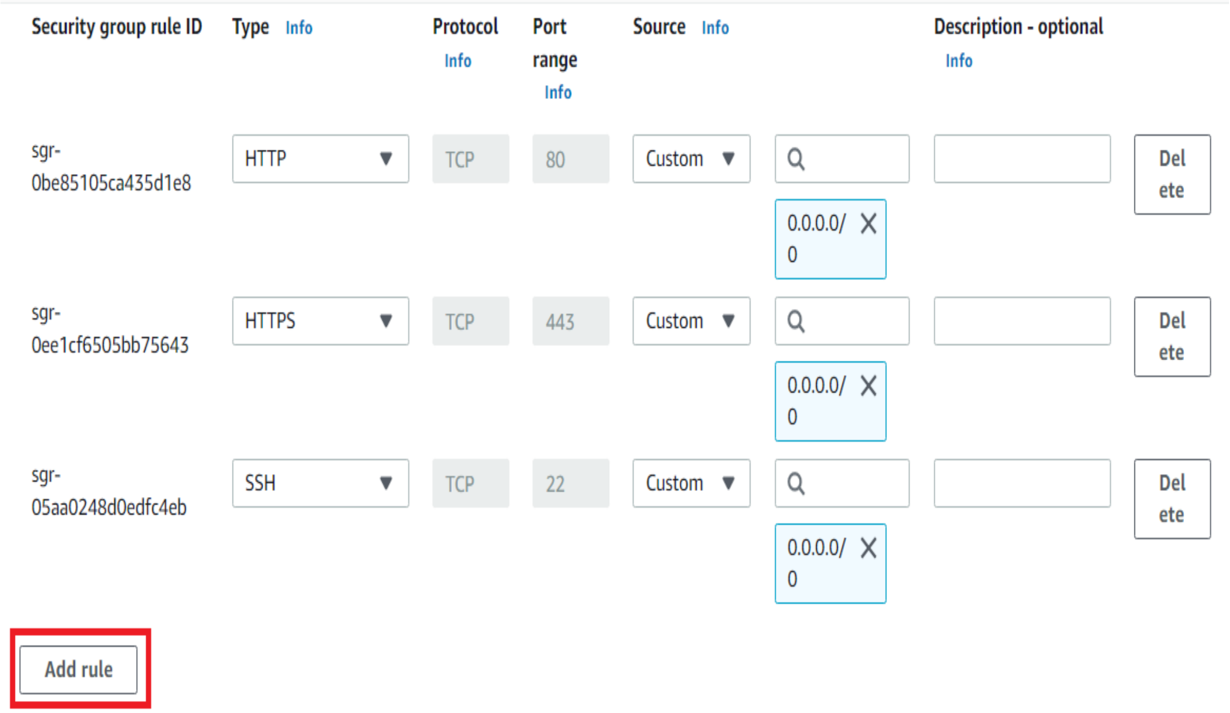


You can now check network connectivity with Reachability Analyzer

Inbound rules (3)

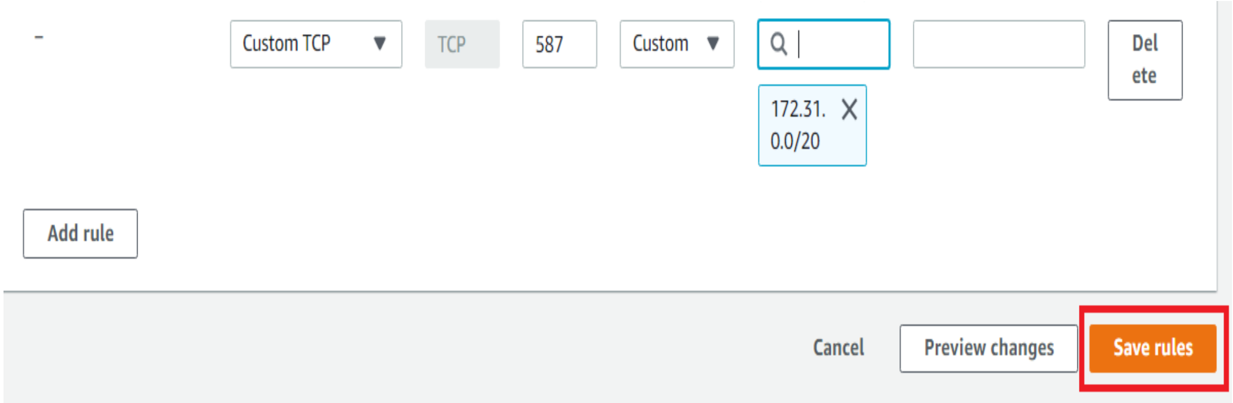
□	Name	Security group rule...	IP version	Type
□	–	sgr-0be85105ca435d1...	IPv4	HTTP
□	–	sgr-0ee1cf6505bb75643	IPv4	HTTPS
□	–	sgr-05aa0248d0edfc4eb	IPv4	SSH

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

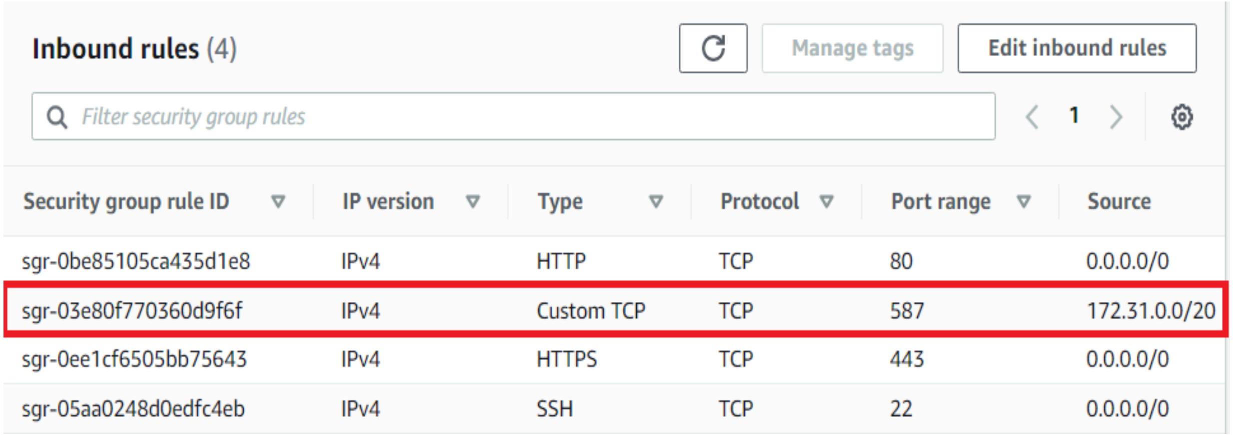


Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-0be85105ca435d1e8	HTTP ▼	TCP	80	Custom ▼	0.0.0.0/0		Delete
sgr-0ee1cf6505bb75643	HTTPS ▼	TCP	443	Custom ▼	0.0.0.0/0		Delete
sgr-05aa0248d0edfc4eb	SSH ▼	TCP	22	Custom ▼	0.0.0.0/0		Delete

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 ▼	172.31.0.0/20		Delete



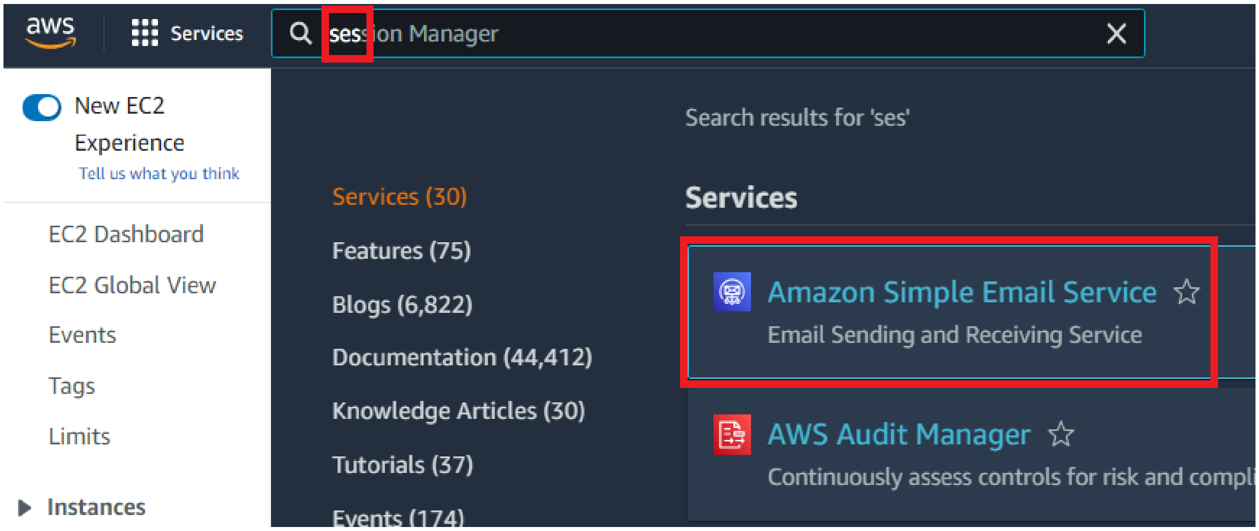
Inbound rules (4)

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

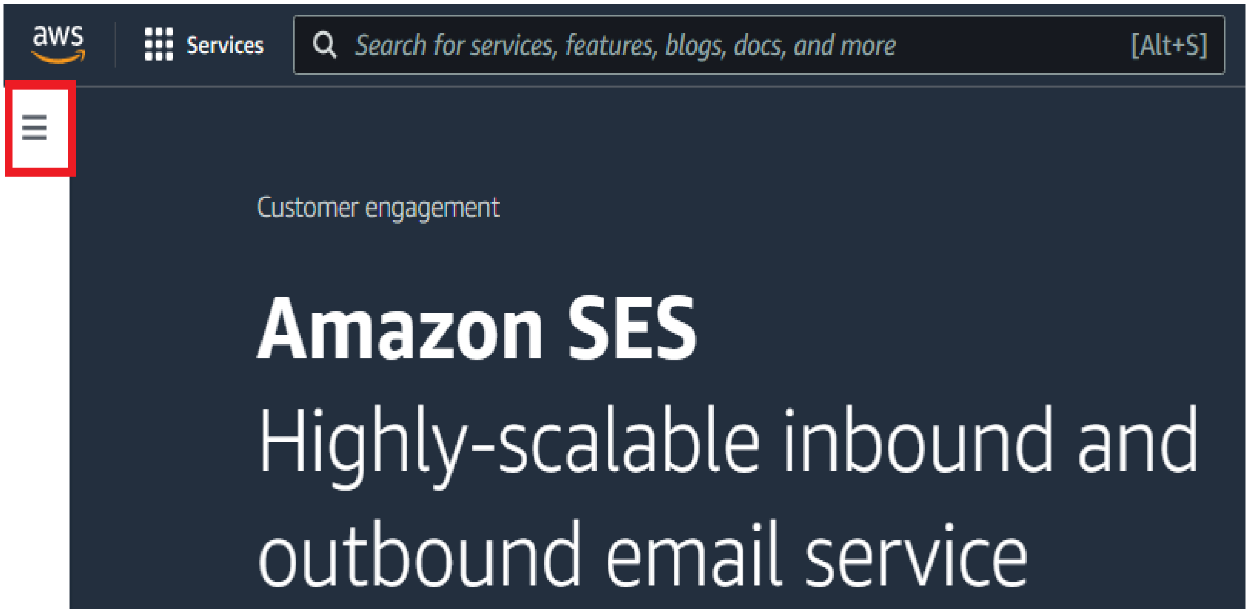
Create Verified Identity

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.

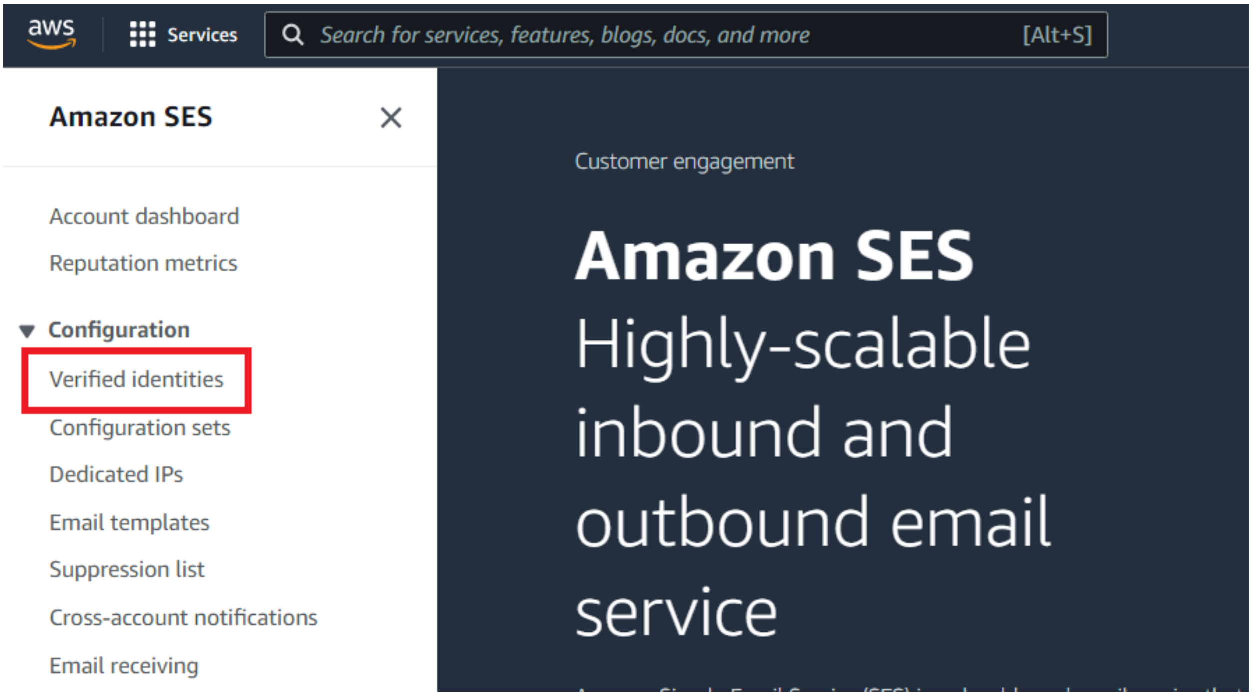
To access the SES service, at the top of the screen, type **ses** in the search bar and select **Amazon Simple Email Service**.



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

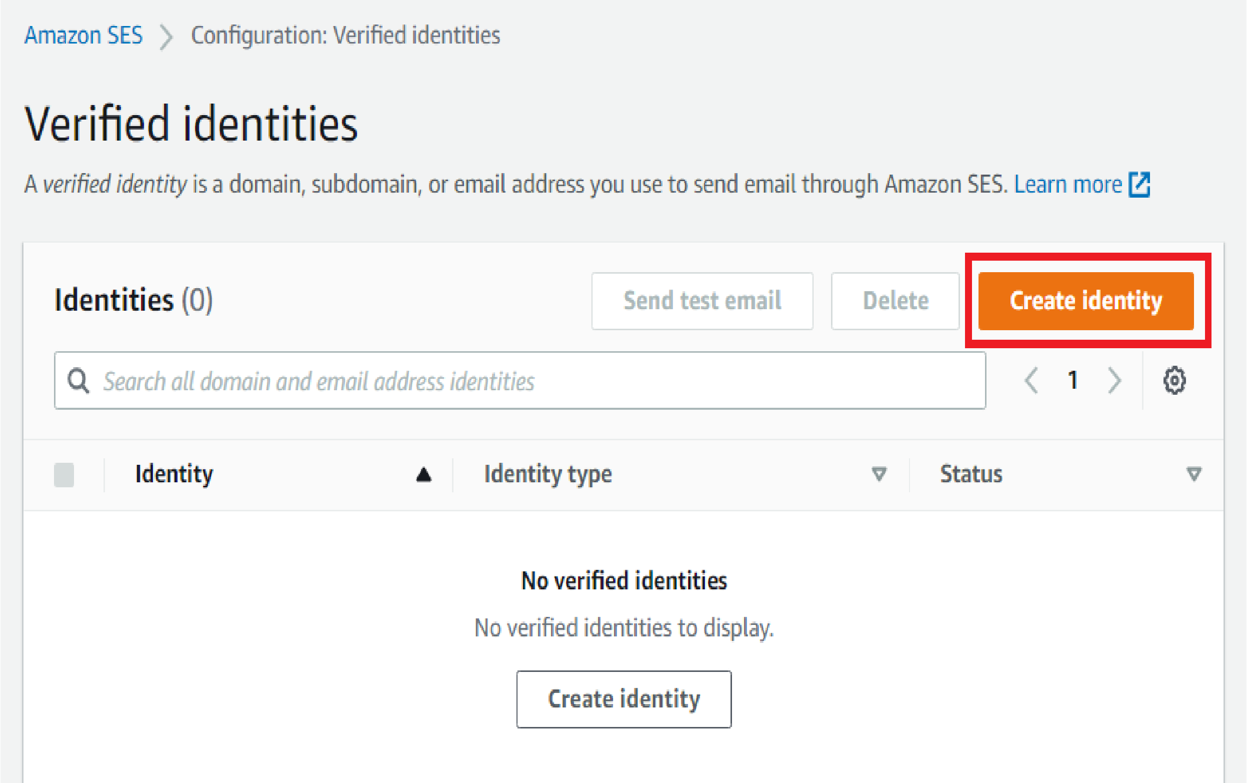

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Customer engagement
Amazon SES
Highly-scalable inbound and outbound email service

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



Amazon SES
Highly-scalable inbound and outbound email service

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



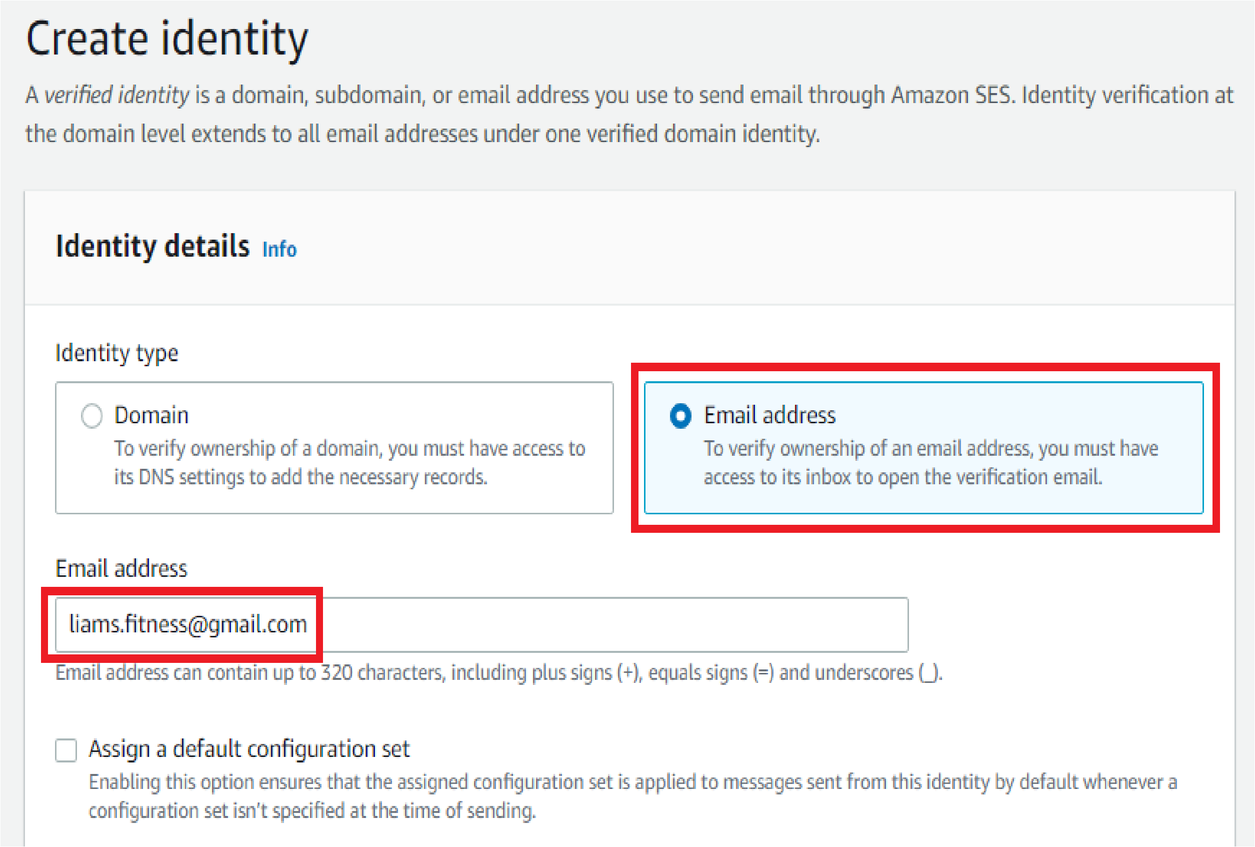
Verified identities

A *verified identity* is a domain, subdomain, or email address you use to send email through Amazon SES. Learn more

No verified identities

No verified identities to display.

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

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.

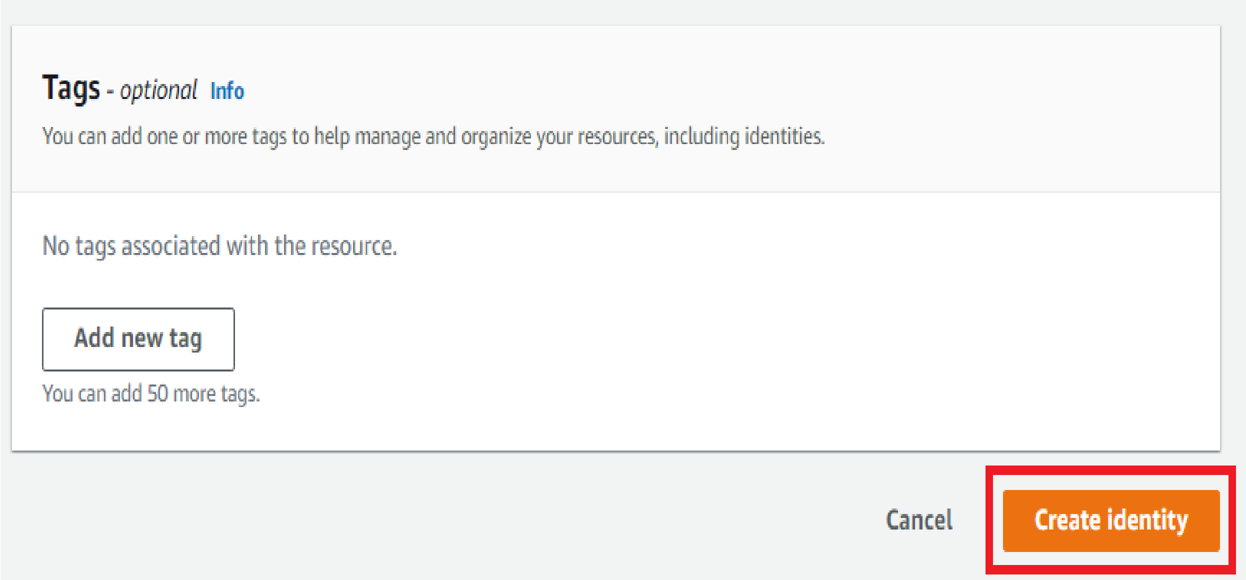
Email address

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**



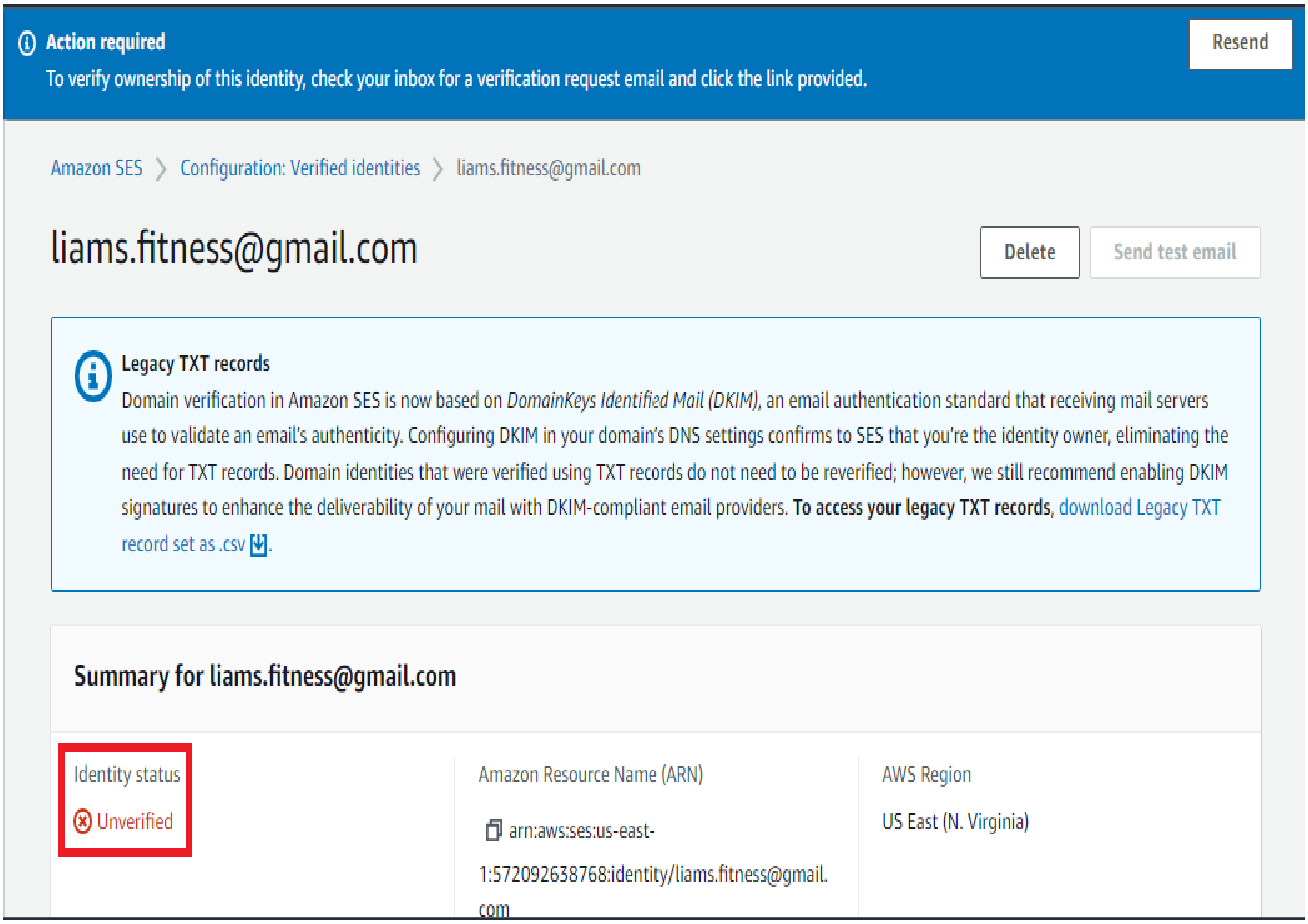
Tags - *optional*

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

No tags associated with the resource.

You can add 50 more tags.

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

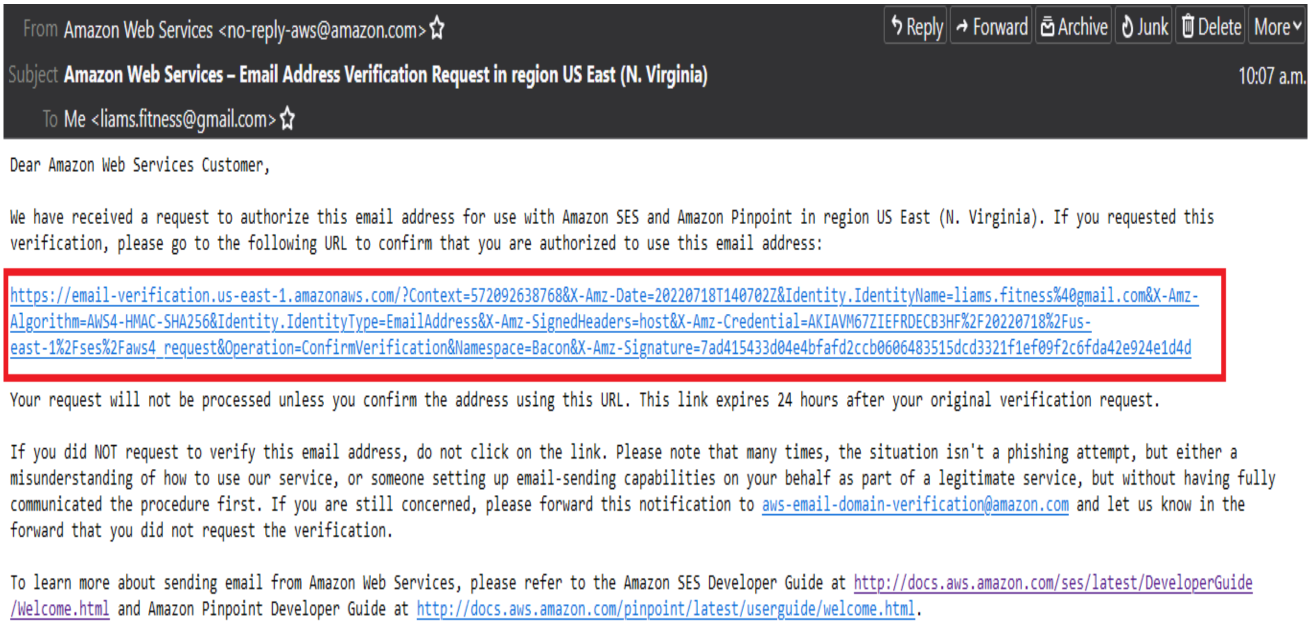
Legacy TXT records

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>

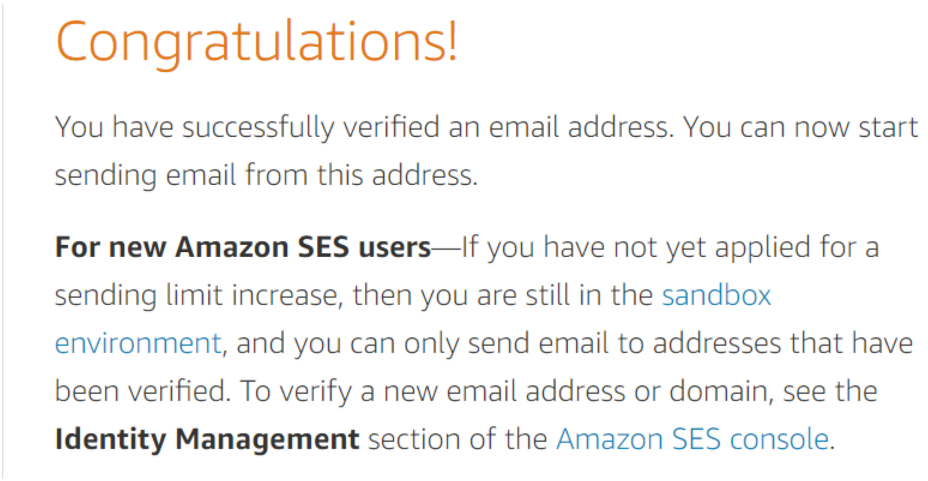
Subject **Amazon Web Services – Email Address Verification Request in region US East (N. Virginia)**

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
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 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.

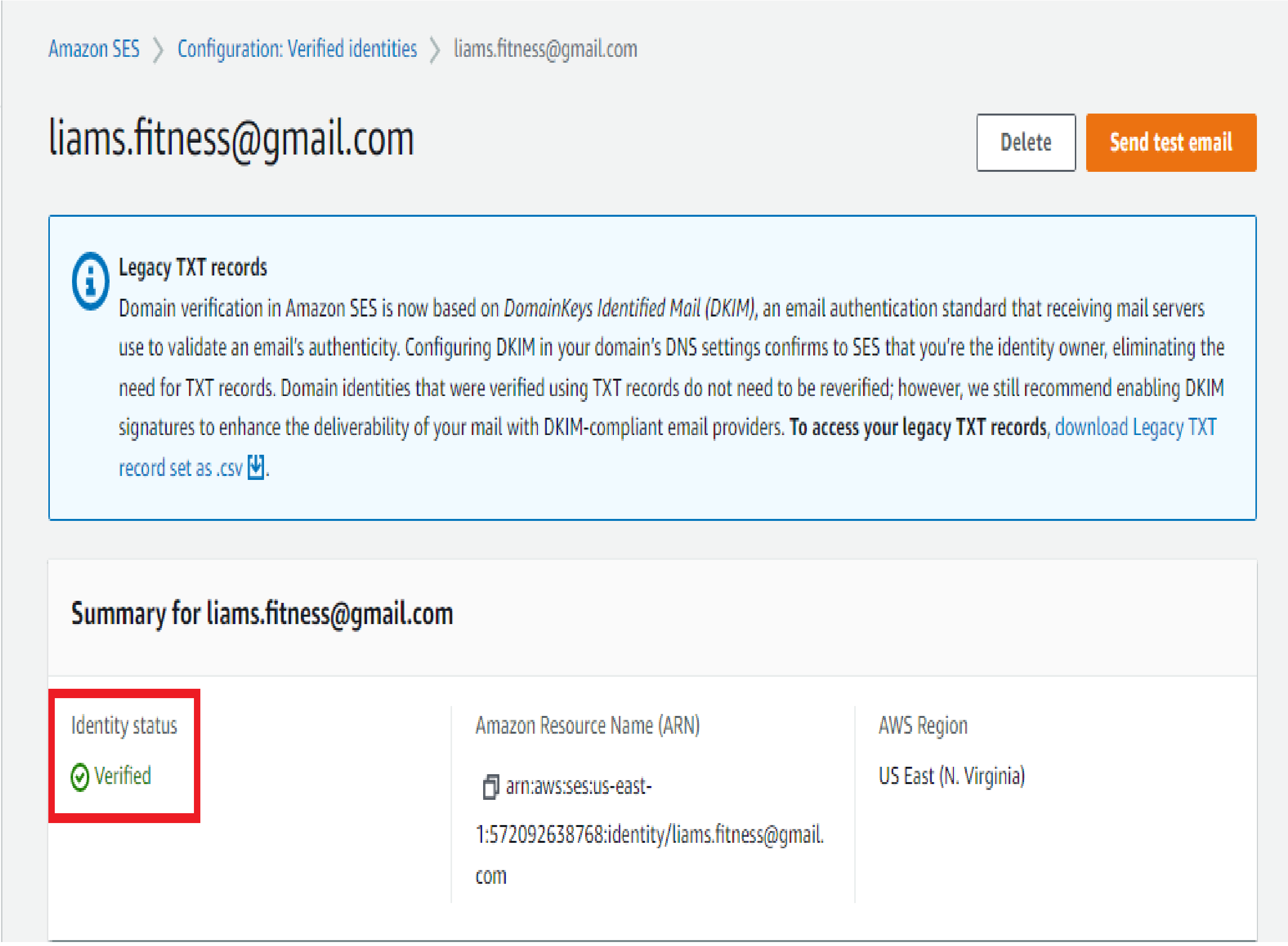


Congratulations!

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.



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

liams.fitness@gmail.com

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

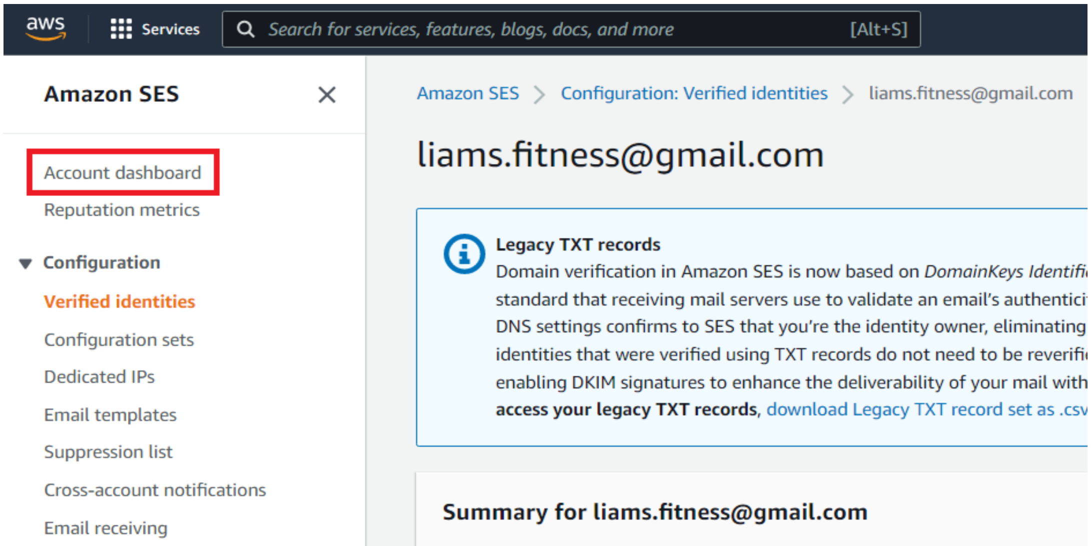
Identity status	Amazon Resource Name (ARN)	AWS Region
✓ Verified	arn:aws:ses:us-east-1:572092638768:identity/liams.fitness@gmail.com	US East (N. Virginia)

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**

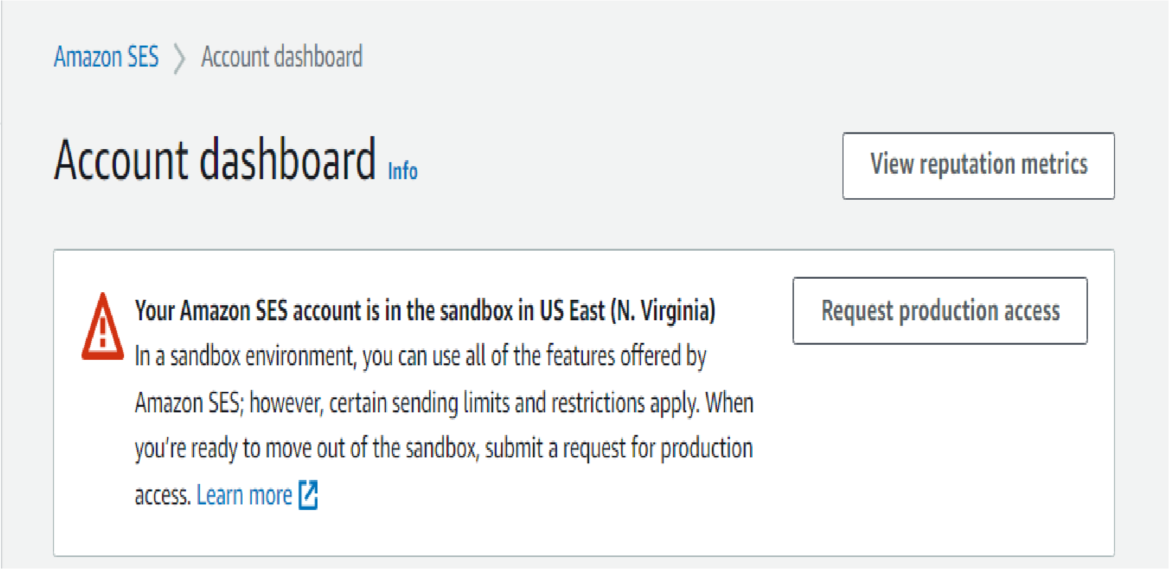


liams.fitness@gmail.com

Legacy TXT records
Domain verification in Amazon SES is now based on *DomainKeys Identifi*
standard that receiving mail servers use to validate an email's authentici
DNS settings confirms to SES that you're the identity owner, eliminating
identities that were verified using TXT records do not need to be reverifi
enabling DKIM signatures to enhance the deliverability of your mail with
access your legacy TXT records, download Legacy TXT record set as .csv

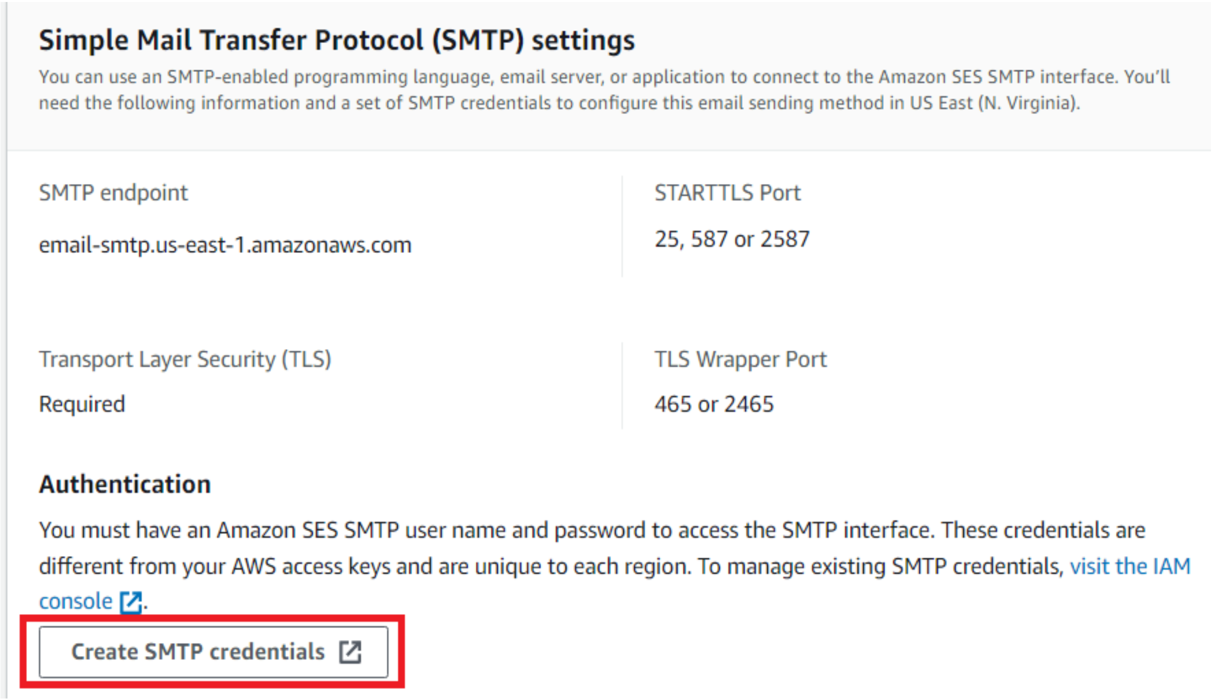
Summary for liams.fitness@gmail.com

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



Your Amazon SES account is in the sandbox in US East (N. Virginia)
In a sandbox environment, you can use all of the features offered by Amazon SES; however, certain sending limits and restrictions apply. When you're ready to move out of the sandbox, submit a request for production access. Learn more

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

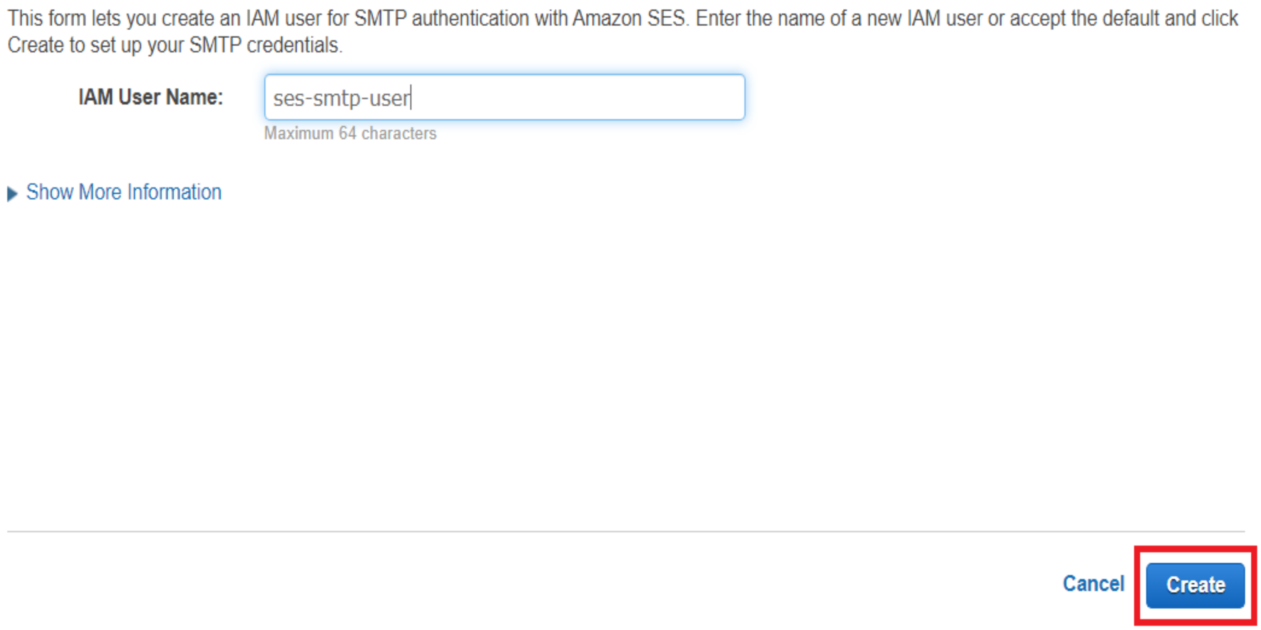
TLS Wrapper Port

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.

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

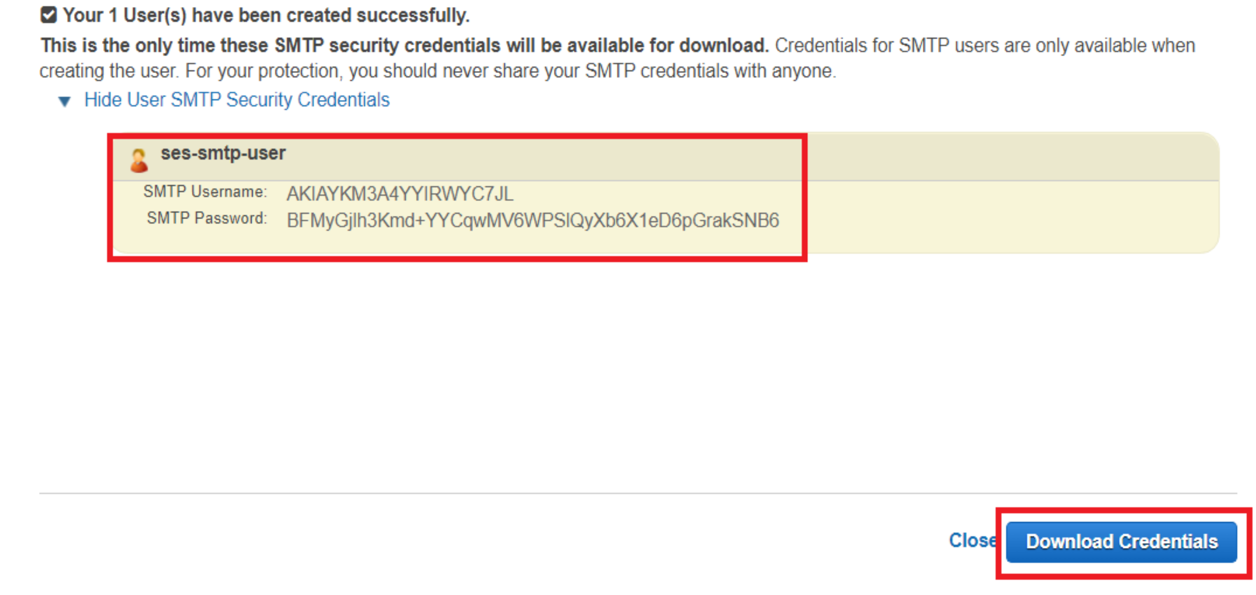


This form lets you create an IAM user for SMTP authentication with Amazon SES. Enter the name of a new IAM user or accept the default and click Create to set up your SMTP credentials.

IAM User Name: ses-smtp-user

Maximum 64 characters

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

ses-smtp-user

SMTP Username: AKIAYKM3A4YYIRWYC7JL

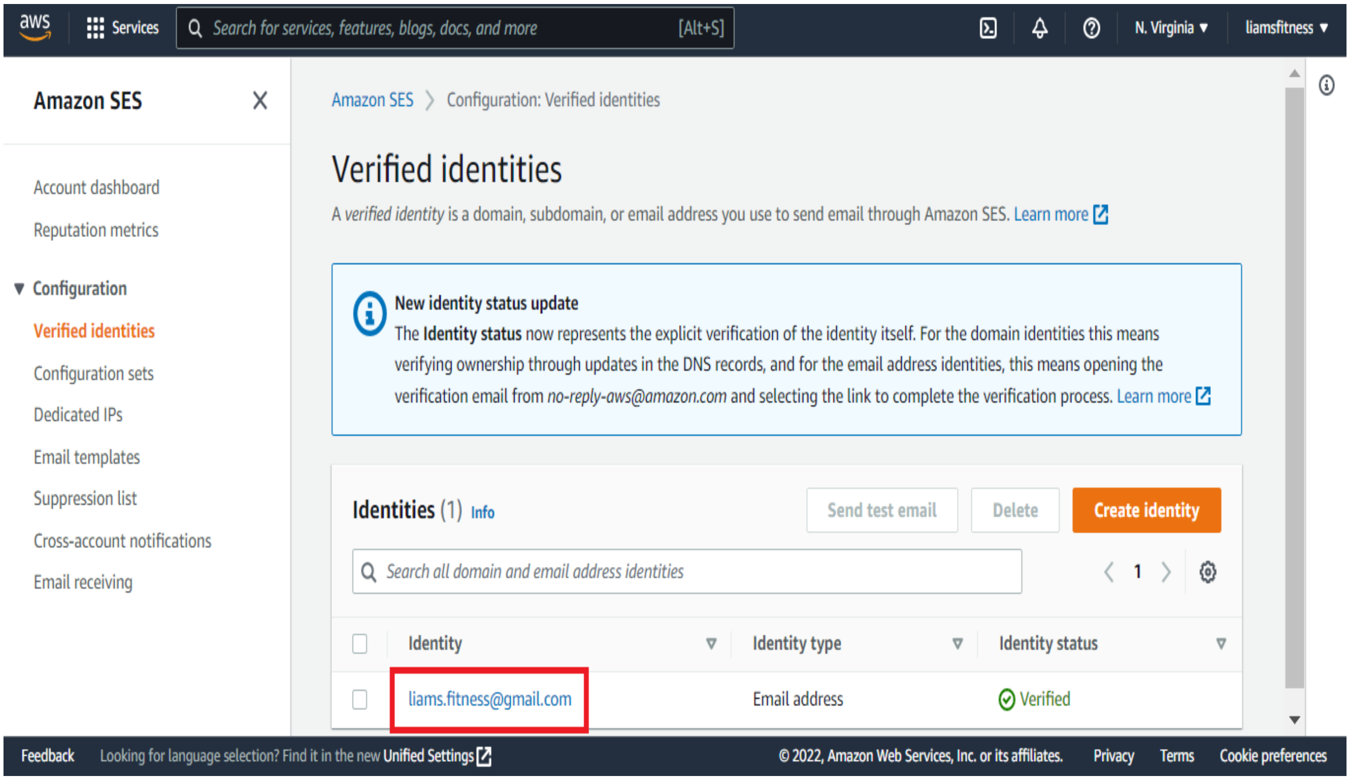
SMTP Password: BFMyGjlh3Kmd+YYCqwMV6WPSlQyXb6X1eD6pGrakSNB6

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

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.



Verified identities

A *verified identity* is a domain, subdomain, or email address you use to send email through Amazon SES. Learn more

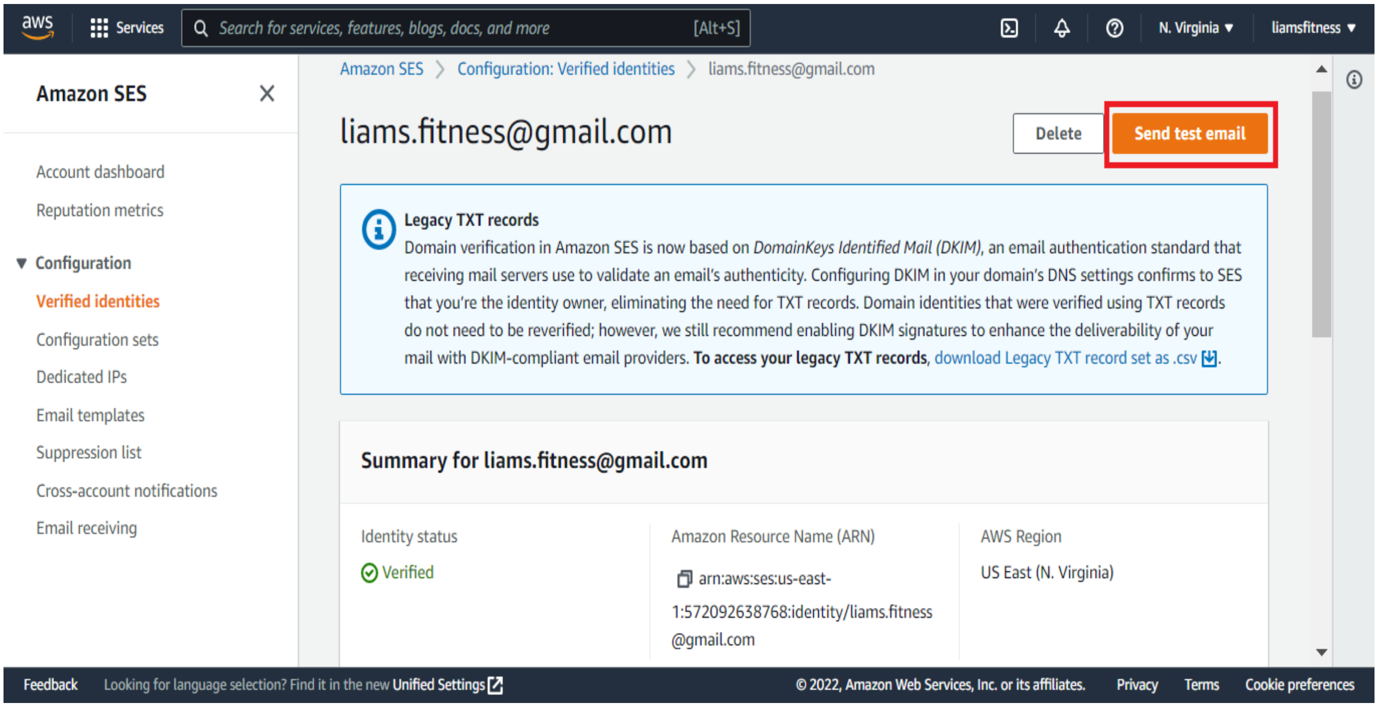
New identity status update

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

	Identity	Identity type	Identity status
□	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**


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
N. Virginia ▾
liamsfitness ▾
Amazon SES > Configuration: Verified identities > liams.fitness@gmail.com
Amazon SES
Account dashboard
Reputation metrics
▾ Configuration
Verified identities
Configuration sets
Dedicated IPs
Email templates
Suppression list
Cross-account notifications
Email receiving
Delete
Send test email
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

liams.fitness@gmail.com

Legacy TXT records

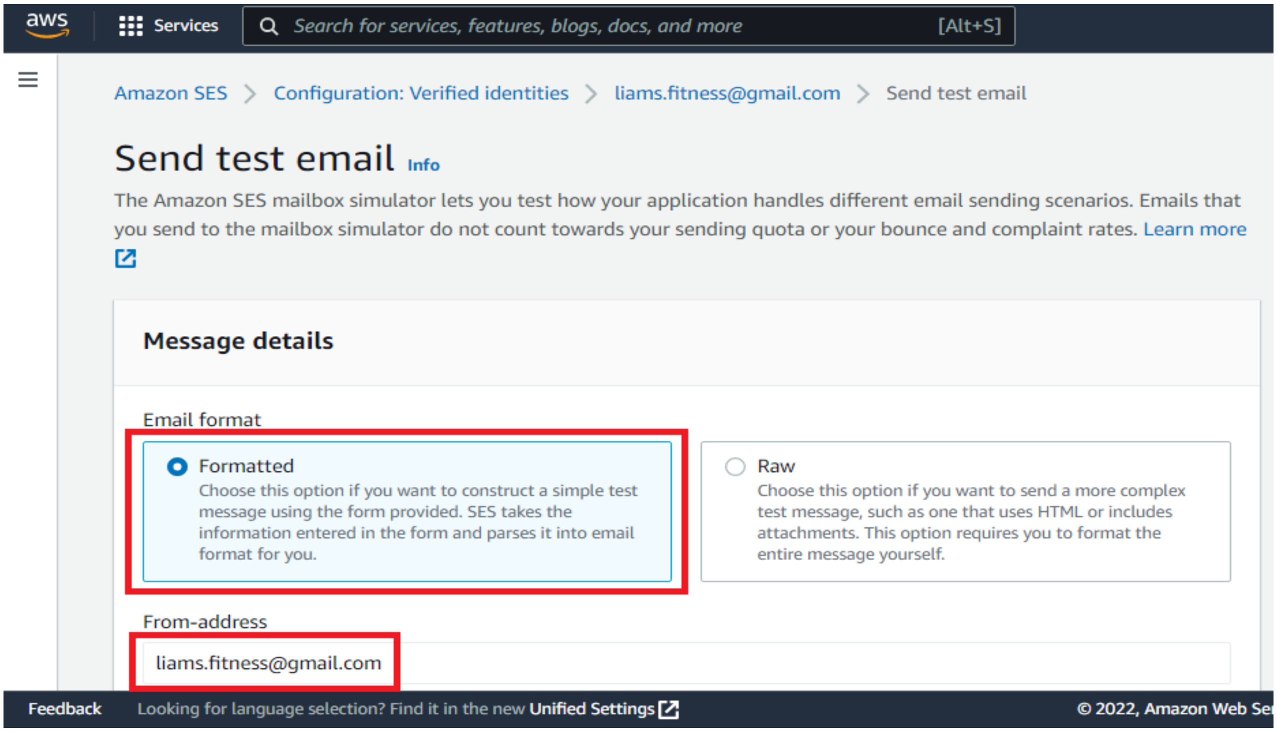
Domain verification in Amazon SES is now based on *DomainKeys Identified Mail (DKIM)*, an email authentication standard that receiving mail servers use to validate an email's authenticity. Configuring DKIM in your domain's DNS settings confirms to SES that you're the identity owner, eliminating the need 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
✓ 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.


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Amazon SES > Configuration: Verified identities > liams.fitness@gmail.com > Send test email
Info
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Se

Send test email

The Amazon SES mailbox simulator lets you test how your application handles different email sending scenarios. Emails that you send to the mailbox simulator do not count towards your sending quota or your bounce and complaint rates. Learn more

Message details

Email format

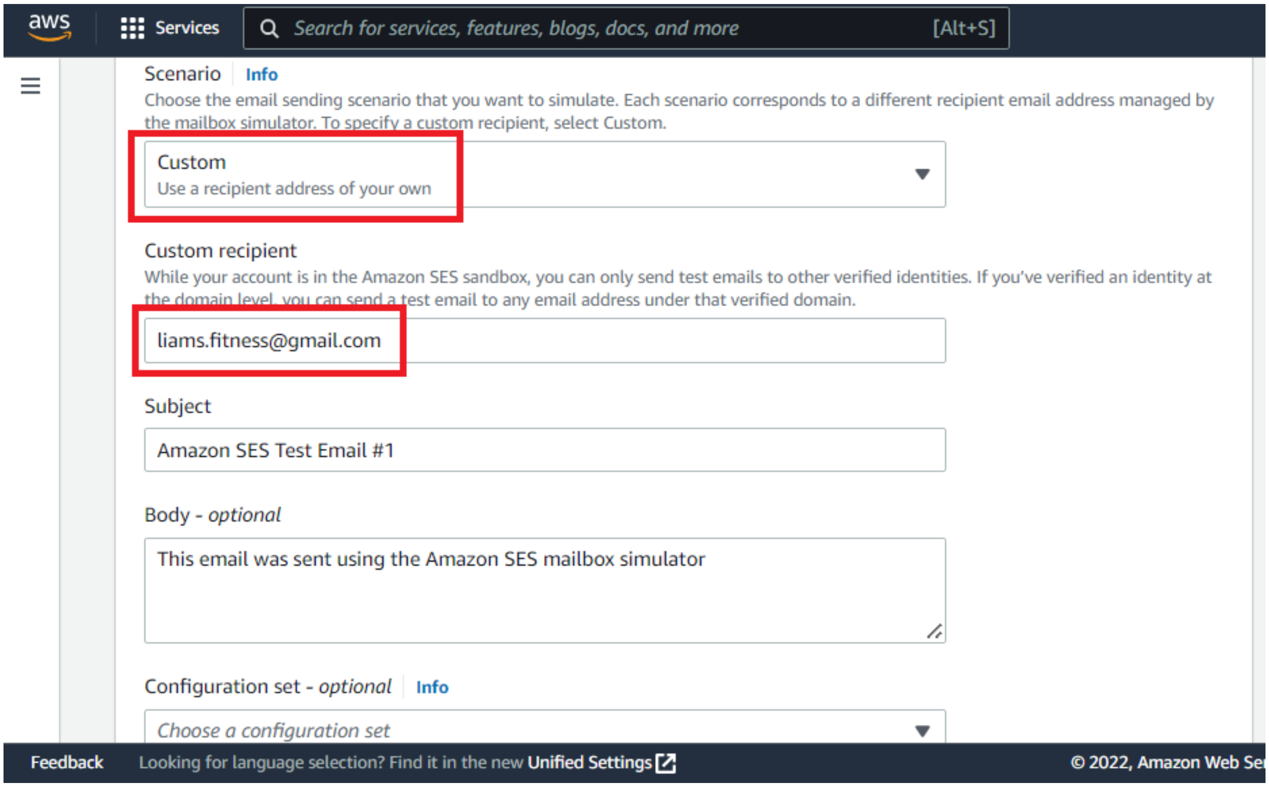
● Formatted
Choose this option if you want to construct a simple test message using the form provided. SES takes the information entered in the form and parses it into email format for you.

○ Raw
Choose this option if you want to send a more complex test message, such as one that uses HTML or includes attachments. This option requires you to format the entire message yourself.

From-address

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.



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*

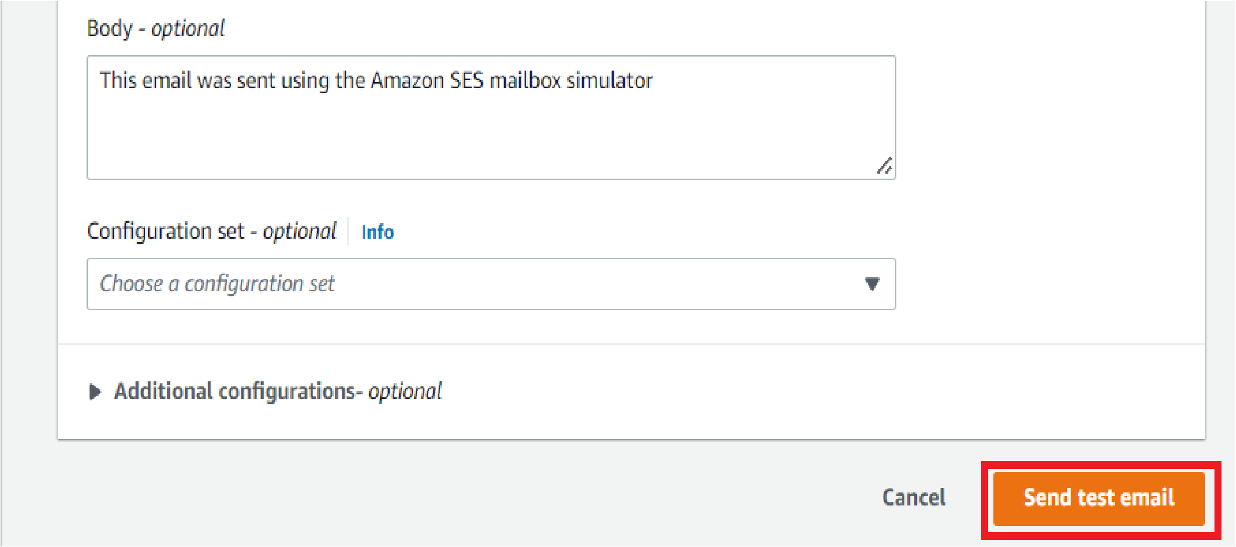
This email was sent using the Amazon SES mailbox simulator

Configuration set - *optional* Info

Choose a configuration set

Feedback
Looking for language selection? Find it in the new **Unified Settings**
© 2022, Amazon Web Se

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



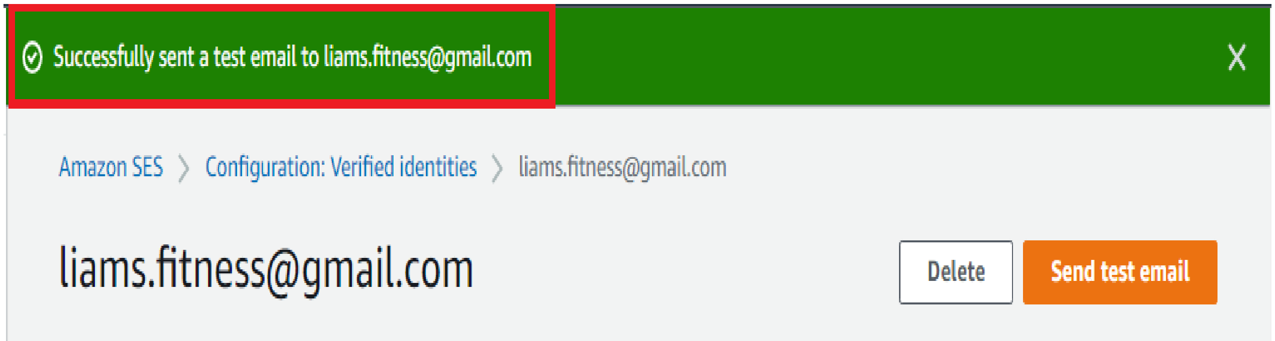
Body - *optional*

This email was sent using the Amazon SES mailbox simulator

Configuration set - *optional* Info

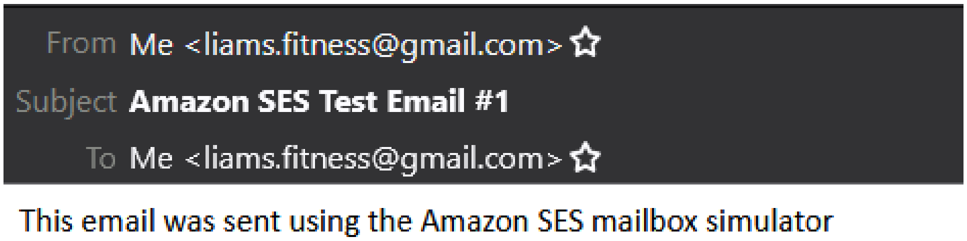
Choose a configuration set

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


Successfully sent a test email to liams.fitness@gmail.com

liams.fitness@gmail.com

I can confirm receipt by checking my email client:


From Me <liams.fitness@gmail.com>

Subject **Amazon SES Test Email #1**

To Me <liams.fitness@gmail.com>

This email was sent using the Amazon SES mailbox simulator

I hope you've enjoyed this tutorial.

We successfully configured the components required by an EC2 to use Amazon SES:

- A verified identity (email address)
- SMTP credentials to access the Amazon SES SMTP interface from an EC2
- Inbound Rule for port 587 added to security group to allow email transmission from an EC2

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.

Back to Top