<https://aws.amazon.com/blogs/messaging-and-targeting/forward-incoming-email-to-an-external-destination/>

Step 1: setup domain and verify

Step 2: create AWS S3 bucket (<https://console.aws.amazon.com/s3/>.)

Tutorial on S3: <https://docs.aws.amazon.com/AmazonS3/latest/gsg/SigningUpforS3.html>

<https://console.aws.amazon.com/iam/home#/home> - awsAccountID

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/add-bucket-policy.html> - add policy

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "AllowSESPuts",

"Effect": "Allow",

"Principal": {

"Service": "ses.amazonaws.com"

},

"Action": "s3:PutObject",

"Resource": "arn:aws:s3:::<bucketName>/\*",

"Condition": {

"StringEquals": {

"aws:Referer": "<awsAccountId>"

}

}

}

]

}

Step 3: IAM policy

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"logs:CreateLogStream",

"logs:CreateLogGroup",

"logs:PutLogEvents"

],

"Resource": "\*"

},

{

"Sid": "VisualEditor1",

"Effect": "Allow",

"Action": [

"s3:GetObject",

"ses:SendRawEmail"

],

"Resource": [

"arn:aws:s3:::<bucketName>/\*",

"arn:aws:ses:<region>:<awsAccountId>:identity/\*"

]

}

]

}

Bucket name, region, account id

Step 4: lambda

Python 3.7

Choose iam role earlier

Environment variables

Basic - Timeout value to 30 seconds

Step 5: sns topic

Step 6: receipt rule set

Add s3 action + lambda (event)

Under **Recipients**, specify the incoming email address or domain for which you want to set up a receipt rule.

<https://bravokeyl.com/how-to-set-up-email-forwarding-with-amazon-ses/#Create-a-Lambda-function-to-forward-recieved-email>

Bounces:

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/notifications-via-email.html>

<https://medium.com/quick-code/how-to-handling-bounced-and-complaint-notification-in-aws-within-15-minutes-827972207484> (better)

Lambda Policy

{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Action": [  
 "logs:CreateLogGroup",  
 "logs:CreateLogStream",  
 "logs:PutLogEvents"  
 ],  
 "Resource": "arn:aws:logs:\*:\*:\*"  
 },  
 {  
 "Effect": "Allow",  
 "Action": "ses:SendRawEmail",  
 "Resource": "\*"  
 },  
 {  
 "Effect": "Allow",  
 "Action": [  
 "s3:GetObject",  
 "s3:PutObject"  
 ],  
 "Resource": "arn:aws:s3:::S3-BUCKET-NAME/\*"  
 }  
 ]  
}

arn:aws:s3:::shsu-bucket-inspire

email rule set:

1. For **Rule Details**, use the following procedure to choose settings.
   1. For **Rule Name**, type a name for the receipt rule. The name must contain less than 64 alphanumeric, hyphen (-), underscore (\_), and period (.) characters. The name must start and end with a letter or number.
   2. If you want to enable the receipt rule, leave the **Enabled** option selected.
   3. If you want Amazon SES to reject any incoming emails that are not sent over a connection that is encrypted with Transport Layer Security (TLS), select **TLS**.
   4. If you want Amazon SES to scan incoming emails for spam and viruses, select **Enable Spam and Virus Scanning**.
2. For **Rule Set**, choose an existing receipt rule set or click **Create New Rule Set**.
3. For **Rule Position**, choose where to place the receipt rule in the ordered list of receipt rules. The receipt rules are evaluated sequentially.

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/receiving-email-receipt-rules.html>

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-smtp.html>

Metrics:

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/monitor-sending-activity.html>

Testing:

<https://docs.aws.amazon.com/ses/latest/DeveloperGuide/mailbox-simulator.html>