Amazon Simple Email Service

Content Prepared By: Chandra Lingam, Cotton Cola Designs LLC

Amazon Simple Email Service

Reliable, Scalable, Inexpensive Email Service

Send and Receive Emails

Pay as you go

Typical Usage

- Marketing Emails
- Transactional Emails – Order Confirmation, Shipping Status, Password Resets…
- Notifications – Application Errors/Alerts, Health Reports, Workflow updates
- Receiving Emails – Receive emails and trigger custom processing and storage

Email Sending Process

Figure: SES Email Sending Process

Spam or Legitimate?

Deliverability - Likelihood of email delivered to inbox instead of marked as spam or blocked

Reputation – Measure of confidence that IP Address, Email Address or Sending Domain is not the source of spam

SES – High Deliverability

SES provides high deliverability by maintaining a strong reputation with ISPs/mailbox providers

Maximize Deliverability

- Comply with industry standard authentication protocols
- SES Offers Dedicated IP Address to establish reputation of the IP address
- Track Email Metrics
- Filters for Virus, Malware
- Sending Limits

Reputation

Reputation is a measure of confidence that IP Address, Email Address or Sending Domain is not the source of spam

- SES maintains a strong reputation with ISPs so that ISPs deliver emails to the recipients inboxes
- You need to maintain a trusted reputation with SES by sending high quality content
- SES increases sending limits as your reputation become more trusted
- Excessive bounces or complaints can impact reputation and SES may lower sending limits or terminate account

Verification

- Easy to spoof emails
- To maintain trust between ISP and SES, SES requires you to verify all sending email addresses
- Verify through SES console or using API
- Verify entire domains
- New accounts are in Sandbox and you are required to verify your recipient address
- You can use SES mailbox simulator to test various scenarios

Authentication

- ISP/Mailbox providers evaluate if email is legitimate
- Authentication is one way to confirm the source of an email – provide evidence that you are the owner and your emails are not modified in-transit
- ISPs can confirm the Identity of Sender using:
    - Sender Policy Framework (SPF)
    - Domain Keys Identified Mail (DKIM)
- Comply with Domain Based Message Authentication, Reporting and Conformance (DMARC) protocol

Sender Policy Framework (SPF)

- SPF is designed to combat email spoofing
- Domain owners identify which mail servers are authorized to send emails for the domain
- Specified as a DNS resource record in domain’s DNS server (TXT records with IP Addresses listed)
- To pass SPF Check:
    - Use default MAIL FROM domain of SES (no need to publish SPF) as SES already has a SPF
    - Use your domain and publish SPF in DNS server

DomainKeys Identified Mail (DKIM)

- Sender signs the messages (Cryptographic signing)
- Protects against unauthorized tampering of messages during transit
- ISPs cross checks the signature against Sender’s public key to detect tampering
- Sender’s Public Key is published in Sender’s DNS records
- SES can automatically add signatures when you setup your domain (or) you can add your own DKIM signature

DMARC Compliance

- Domain based message authentication, Reporting and Conformance (DMARC) is an email authentication protocol
- Uses SPF and DKIM to detect email spoofing
- Email can comply with DMARC through SPF or through DKIM
- Best practice is to setup email sending to comply with both methods

Sending Limits

- ISPs may block emails if they detect sudden, unexpected spike in email volumes
- SES enforces a sending limit to regulate number of emails (Sending Quota: max per day) and the rate at which they are sent (Max Send Rate: max per second)
- Sending Limits help protect your trustworthiness with the ISP
- Sending Limits start small and gradually increase – if they are acceptable to ISPs

SES Sandbox

- To help protect customers from fraud and abuse
- To help establish your trustworthiness with ISPs, Email Recipients
- New SES are initially placed in a Sandbox environment
    - Send email to SES mailbox simulator
    - Send email to verified recipient address and domains
    - Max 200 messages in 24 hour period
    - Max one message per second rate
    - Region specific limits
- To move out of Sandbox and to increase limits, you need to open a support case

Content Filtering

- ISPs use content filtering to detect spams
- SES uses content filters to ensure SES accounts are not spammers
- Your reputation with SES will be negatively affected if SES content filters detect spams in your messages
- If a message is infected with virus, SES rejects it

Feedback

- Notifications
  - Bounces: ISP -> SES -> You
  - Complaints: ISP -> SES -> You
  - SES has complaint feedback loop with ISPs
- Notifications can be through
  - SNS topics – Bounces/Complaints/Successful
  - Emails – Bounces/Complaints
- Usage Statistics
  - Failed Deliveries, Successful Deliveries, Complaints, Bounces, Virus infected rejects, Sending limits

Monitoring

Email Sending Event Metrics:

- Bounces : Hard – recipient not known. Soft – intermittent issues or problem with recipient inbox
- Complaints – Email marked as spam
- Sends – API call to SES was successful. SES will attempt to deliver the email
- Rejected Emails – SES rejected email due to virus
- Deliveries – SES successfully delivered email to recipient’s mail server

Dedicated and Shared IP Address

SES can use its own IP Addresses that are shared among customers

- *Cost Effective*

SES can reserve IP address for your dedicated use:

- *Suitable for large senders, requires minimum daily volume commitment, more-expensive*

Receiving Emails

- Configurable receiving options based on recipient address and/or senders IP address
    - Accept or Reject emails
- Processing Options for received emails:
    - Store in S3 with optional SES/KMS encryption of messages
    - Trigger custom AWS Lambda code
    - Publish notifications to SNS
    - Bounce messages
    - Specified using Receipt Rules

Multiple interfaces for sending emails

- SES Console
- Simple Mail Transfer Protocol (SMTP) interface
- SES API
- AWS SDKs
- AWS CLI

Credentials

- IAM Credentials – for accessing SES API/SDK/CLI, use access key and secret access key. For accessing management console use IAM user/password
- SES SMTP Credentials – for accessing SES SMTP Interface

Integration

SES Seamlessly integrates with other AWS services such as EC2, Lambda, SNS, IAM, S3 and so forth

Pricing

- Free Tier
    - EC2 users can send 62,000 messages/month from their EC2 instance
    - Receive 1,000 messages/month
    - Does not expire after 1 year
    - Data Transfer, mail chunk (256KB chunks), attachment fees, apply

Pricing

- Email Messages
  - $0.10 per 1,000 messages
  - $0.12 per GB of attachments sent
- Dedicated IP Address
  - $25 per month
- Mail Chunks - $0.09 per 1,000 mail chunks
  - Received mail is computed in terms of 256KB chunks