How to Add SPF and DKIM Records to Amazon Route 53

Adding SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail) records to your Route 53 hosted domain is an essential step to improve email deliverability and security. These records help verify the authenticity of your email messages, reducing the chances of your emails being marked as spam. Here's a step-by-step guide on how to add SPF and DKIM records for a domain hosted on Route 53:

1. Log in to your AWS Route 53 Console:

- Go to the AWS Management Console (https://aws.amazon.com/).
- Sign in to your AWS account.
- Navigate to the Route 53 service.

2. Select Your Domain:

- In the Route 53 dashboard, select the domain for which you want to add SPF and DKIM records.

3. Add SPF Record:

a. SPF records specify which servers are authorized to send email on behalf of your domain. To add an SPF record:

- In the Route 53 dashboard for your domain, click on "Create Record Set" or "Add Record Set."
- Leave the "Name" field blank to create the SPF record for the root domain (e.g., example.com).
- Set the "Type" to "TXT."
- In the "Value" field, enter your SPF record. Here's an example of an SPF record:
  arduino Copy code
  `"v=spf1 include:amazonses.com ~all"`
- Click "Save Record Set" or the equivalent option to save your SPF record.

4. Add DKIM Record:

a. DKIM records provide a signature for your outgoing emails to verify their authenticity. To set up DKIM:

- In your AWS SES (Simple Email Service) dashboard (if you're using SES), navigate to "Email Sending Domains" and select your domain.
- Follow the instructions provided by SES to create DKIM records. This typically involves adding CNAME records in Route 53 with specific values provided by SES.
- In Route 53, create a CNAME record set with the appropriate DKIM values provided by SES.
- Ensure that the "Name" field matches the DKIM record name provided by SES (e.g., "ses1._domainkey.example.com").
- Set the "Type" to "CNAME."
- In the "Value" field, enter the DKIM value provided by SES.
- Click "Save Record Set" to save your DKIM record.

5. Verify Records:

- After adding SPF and DKIM records, it might take some time for DNS propagation. You can use online DNS checking tools to verify that your records are correctly set up.

6. Test Your Email Configuration:

- Send test emails to various email providers to ensure that your SPF and DKIM records are working correctly. Check the email headers to confirm that SPF and DKIM authentication passed.

7. Monitor and Update:

- Regularly monitor your email deliverability and reputation. Make updates to your SPF and DKIM records as needed, especially if you change email providers or sending servers.

That's it! Adding SPF and DKIM records to your Route 53 hosted domain helps improve email deliverability and security by verifying the authenticity of your email messages.

Revision #3
Created 7 October 2023 10:55:25 by Cindy
Updated 7 October 2023 11:03:58 by Cindy