Advanced Email Setup

Mandril integration with Exim MTA

Hubs are configured to send and receive email directly. However depending on server configuration, some mail servers on the internet may view an email message sent by your hub as SPAM. This can happen for a variety of reasons, ranging from partially setup machines used in development environments, servers that do not have DNS names properly established, MTAs that are not properly configured, etc.

Often you can find and fix specific issues it can help save your hub's email from your users' SPAM folders, but sometimes in cloud environments, your server is assigned an IP address from a pool of addresses where a previous user has used an IP addresses in that range to SPAM in the past, so your IP address itself of your server is blacklisted by various SPAM tracking software packages.

Often using a third party email provider such as Amazon SES or Mandrill can help rescue your outgoing email from your users' SPAM folders. This is an especially important issue for hubs that even occasionally send legitimate mass email to their users.

Setup an account with Mandrill. The free tier of service from Mandrill will allow for up to 12000 email per month with no charges.

Setup

1. Login/sudo to your Debian machine as root. The following command will run you through the standard Exim configuration application. For each of the screens, enter the following:

   % dpkg-reconfigure exim4-config
2. Mail Server configuration (page 1):

   Select “mail sent by smarthost; received via SMTP or fetch mail"
3. Mail Server configuration (page 2):

   For “System mail name:” enter your machine’s domain name
4. Mail Server configuration (page 3):

   For “IP addresses to listen on for incoming SMTP connections:” enter 127.0.0.1
5. Mail Server configuration (page 4):

   For "Other Destinations for which mail is accepted:" leave the field blank
6. Mail Server configuration (page 5):

For "Machines to relay mail for" leave this field blank

7. Mail Server configuration (page 6):

   For "IP address or host name of the Outgoing smarthost" enter:
   smtp.mandrillapp.com::587
8. Mail Server configuration (page 7):

   For "Hide local mail name in outgoing mail?" select <NO>
9. Mail Server configuration (page 8):

   For "Keep number of DNS-queries minimal (DialonDemand)" select <NO>
10. Mail Server configuration (page 9):

    "Delivery method for local mail" select: "mbox format in /var/mail/"
11. Mail Server configuration (page 10):

    "Split configuration into small files" select <YES>
12. Mail Server configuration (page 11):

    "root and postmaster mail recipient" leave blank
13. Create a file /etc/exim4/passwd.client file as root:

    % nano /etc exim4/passwd.client
14. Enter the following line at the end of the file:

    *.mandrillapp.com: SMTPUSERNAME: API KEY

    Note: Go to your mandril app and select the "Settings page from your dashboard to get your SMTP Username and API Key.
15. Make sure the group and permissions are properly set on the passed.client file:

    % chgrp Debian-exim /etc/exim4/passwd.client
    % chmod 640 /etc/exim4/passwd.client

Mandril Integration with Postfix

1. Add the following lines to your /etc/postfix/main.cf:

   # Mandril setup

   # enable SASL authentication
   smtp_sasl_auth_enable = yes

   # tell Postfix where the credentials are stored
   smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
   smtp_sasl_security_options = noanonymous

   relayhost = [smtp.mandrillapp.com]:587
2. Go to your Mandrill App homepage, select 'Settings' from the left hand column.

3. Create a new API Key for your server. Make note of the API Key you created as well as the SMTP credentials at the top of the page.

4. Create a file called */etc/postfix/sasl_passwd* with the following contents:
   [smtp.mandrillapp.com]:587 <SMTP Username>:<API Key>

5. Run: **postmap /etc/postfix/sasl_passwd**

6. Restart postfix: **/etc/init.d/postfix restart**

Note: For even more security, you might also want to setup DKIM and SPF on the host. On Mandril's page, go to 'Settings'->'Domain' Tab. Once you have sent an email or two through Mandrill's system, your server should appear in this list. You'll need to add several DNS TXT records, as well as have Mandrill deliver an email to a local account on your server, there will be a verify link in the email you must vist.

Contact your group's system administrator for details on adding DNS entires for this setup. For the verification email, you can send an email to the root user on your server, then look in the /var/mail/root file. You might need to enable postfix to deliver mail to root.