Authenticated Relay with Postfix

Unix servers generally come with some kind of mail server installed. This is used to send mail generated by the system for log reports, error messages, etc... By default, it goes to the root account on the local server, but this requires a technician to log into each server and manually check mail. It is much better to have all mail forwarded to one or more e-mail accounts. See this article for instructions on how to set that up.

Long ago, in a galaxy far, far away, we could set up a central mail server to simply relay all e-mail from any random server. We would set up the root user on each server to actually be an e-mail account on a centralized machine, then check that one account. Then, the spammers got involved, started using these *open relays* to send out junk mail, and we had to turn them off.

Now, we can tell a centralized mail server to relay for some tightly controlled servers which we trust, but a better answer is to have relaying only done via authenticated connections. The remote machines actually send a username and password to the centralized (relay) server, then we can feel more confident the traffic is legitimate. This is used, for example, to get log and error messages from the satellite servers to the correct technician.

1. Create an e-mail account on the central (relay server). This account can, if you want, only be used to authenticate the sending of the mail forwarded to it by the satellite servers. It does not (and usually is not) the same as the account the root mail from the satellite servers are going to.
    1. Use some kind of weird e-mail address to decrease crackers. Just generate a random string someplace that is a valid e-mail account.
    2. Your password is never used by a human, so it can be as complex and difficult to remember as you like.
    3. If possible, you can disable SMTP reception on this account which increases security. The account is only used for authentication.
2. On each satellite server, do the following
3. edit /etc/postfix/main.cf
    1. Add/Edit relayhost line to point to main server
    2. Add/Edit smtp_sasl_password_maps line to point to file with credentials
4. Create credentials file
    1. Add line to /etc/postfix/sasl/sasl_password. This contains two fields as followed (separated by a space)
        1. name of server, exactly as entered in relayhost line
        2. a space as a delimiter
        3. login credentials, separated by a colon
            1. username on target server
            2. a colon as a delimitere
            3. password for username on target server
5. Generated the hash file with the postmap command
    1. *postmap /etc/postfix/sasl/sasl_passwd*
6. Verify /etc/postfix/sasl/sasl_passwd.db has been create
7. restart postfix (service postfix restart)
8. verify mail can be sent using whatever program you want.

main.cf_additions

```
# mail host which handles our outgoing traffic for us
relayhost = [smtp.example.com]:587
# credentials for relayhost are in this file
smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd
```

sasl_passwd

```
[smtp.example.com]:587 sysinfo@example.com:someValidPassword
```